
Bitdefender®
GravityZone
INSTALLATIONSHANDBUCH

Bitdefender GravityZone
Installationshandbuch

Veröffentlicht 2015.06.09



Inhaltsverzeichnis

Vorwort

Dieses Handbuch richtet sich an Netzwerkadministratoren, deren Aufgabe es ist, GravityZone in ihrem Unternehmen zu installieren, sowie an Unternehmensadministratoren, die Informationen über die Anforderungen und verfügbaren Sicherheitsmodule von GravityZone benötigen.

In diesem Dokument wird erklärt, wie Sie die GravityZone-Lösung und ihre Sicherheitsagenten auf sämtlichen Arten von Endpunkten in Ihrem Unternehmen installieren und konfigurieren können.

1. Konventionen in diesem Handbuch

Typografie

In diesem Handbuch werden verschiedene Schriftarten verwendet, um die Lektüre zu erleichtern. In der unten stehenden Tabelle erfahren Sie, was welche Schriftart bedeutet.

Erscheinungsbild	Beschreibung
`Beispiel`	Einzugebende Befehle und Syntaxen, Pfade und Dateinamen, Konfigurationen, Dateiausgaben und andere Eingabetexte sind in `nicht-proportionaler` Schrift gedruckt.
http://www.bitdefender.de	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Optionen der Benutzeroberfläche, Stichwörter oder Tastenkombinationen werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

1. ÜBER GRAVITYZONE

GravityZone ist eine Sicherheitslösung für Unternehmen, die speziell auf virtuelle und Cloud-Umgebungen zugeschnitten ist, und bietet Sicherheitsdienste für physische Endpunkte, Mobilgeräte und virtuelle Maschinen in der Private und der Public Cloud sowie für Exchange-Mail-Server.

GravityZone ist ein umfassendes Produkt mit einer zentralen Verwaltungskonsole, die entweder von Bitdefender in der Cloud gehostet oder als virtuelle Appliance innerhalb des Unternehmens installiert wird. Über diese Konsole können von zentraler Stelle aus Sicherheitsrichtlinien für eine beliebige Zahl an Endpunkten erstellt, zugewiesen und verwaltet werden, unabhängig vom Typ und geographischen Ort dieser Endpunkte.

GravityZone bietet Endpunkten (auch Microsoft-Exchange-Mail-Servern) in mehreren Schichten: Viren- und Malware-Schutz mit Verhaltensanalyse, Schutz vor Zero-Day-Attacken, Anwendungssteuerung und Sandbox, Firewall, Gerätesteuerung, Inhaltssteuerung, Phishing- und Spam-Schutz.

1.1. GravityZone-Sicherheitsdienste

GravityZone enthält die folgenden Sicherheitsdienste:

- Security for Endpoints
- Security for Virtualized Environments
- Security for Exchange
- Security for Mobile

1.1.1. Security for Endpoints

Die Lösung bietet unauffälligen Schutz für eine beliebige Anzahl an Windows-, Linux- und Mac-Systemen und setzt dabei auf vielfach ausgezeichnete Malware-Schutz-Technologien kombiniert mit einer Zwei-Wege-Firewall, Angriffserkennung, der Steuerung und Filterung des Internet-Zugriffs, dem Schutz von sensiblen Daten sowie Geräte- und Anwendungssteuerung. Die geringen Ressourcenanforderungen der Software garantieren Leistungsgewinne, und über die Integration mit Microsoft Active Directory lassen sich nicht-verwaltete Arbeitsplatzrechner und Server unkompliziert und automatisch schützen. Die Lösung bietet viele Vorteile gegenüber herkömmlicher Malware-Schutz-Software, da sie vielfach ausgezeichnete Sicherheitstechnologien mit hoher

Benutzerfreundlichkeit und zentraler Verwaltung über das GravityZone Control Center bietet. Proaktive Heuristiken werden eingesetzt, um bösartige Prozesse aufgrund ihres Verhaltens zu erkennen. Dadurch können neue Bedrohungen in Echtzeit erkannt werden.

1.1.2. Security for Virtualized Environments

GravityZone ist die erste wirklich plattformunabhängige Sicherheitslösung für moderne, dynamische Rechenzentren. Sie ist kompatibel mit allen gängigen Hypervisoren von VMware ESXi über Citrix Xen bis hin zu Microsoft Hyper-V. Bitdefender Security for Virtualized Environments macht sich die Ressourcenbündelung virtueller Umgebungen zu Nutze, indem wichtige Sicherheitsvorgänge auf eine zentrale virtuelle Appliance ausgelagert werden. Die Lösung setzt topmoderne Cache-Technologie ein, die gegenüber herkömmlicher Sicherheitssoftware Gewinne in puncto Leistung und Server-Konsolidierung von bis zu 30 % bringt. Security for Virtualized Environments kann mit Plattformen anderer Anbieter wie VMware vCenter oder XenServer integriert werden, um Verwaltungsvorgänge zu automatisieren und so Betriebskosten zu sparen.

1.1.3. Security for Exchange

Bitdefender Security for Exchange bietet Malware-, Spam- und Phishing-Schutz sowie eine Anhang- und Inhaltsfilterung. Die Lösung lässt sich nahtlos mit Microsoft Exchange Server integrieren und schafft so eine Malware-freie E-Mail- und Kollaborations-Umgebung und erhöht damit die Produktivität. Dank mehrfach ausgezeichneter Malware- und Spam-Schutz-Technologie schützt die Software Exchange-Benutzer vor der neuesten und gefährlichsten Malware sowie vor Datendiebstahl.

1.1.4. Security for Mobile

Die Lösung vereint unternehmensweite Sicherheit mit der Verwaltung und Compliance-Überwachung von iPhones, iPads und Android-Geräten durch die zuverlässige Bereitstellung von Software und Updates über die Apple- und Android-Marktplätze. Durch einheitliche Durchsetzung von Sicherheitsrichtlinien auf allen Mobilgeräten können Mitarbeiter ihre eigenen Geräte sicher und kontrolliert im Unternehmensnetzwerk verwenden (BYOD). Zu den Sicherheitsfunktionen gehören Bildschirmsperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch

Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht. So werden die Mobilgeräte zuverlässig kontrolliert und die darauf gespeicherten sensiblen Unternehmensdaten geschützt.

1.2. GravityZone-Architektur

Dank seiner einzigartigen Architektur ist GravityZone extrem skalierbar und kann eine beliebige Anzahl von Systemen schützen. GravityZone kann mehrere virtuelle Appliances und mehrere Instanzen bestimmter Rollen (Datenbank, Kommunikationsserver, Update-Server und Web-Konsole) verwenden, um Verfügbarkeit und Skalierbarkeit auf hohem Niveau zu halten.

Jede Instanz einer Rolle kann auf einer anderen Appliance installiert werden. Eingebaute Lastenverteilungen gewährleisten, dass GravityZone selbst die umfangreichsten Unternehmensnetzwerke zuverlässig schützen kann, ohne Verzögerungen oder Ressourcenengpässe zu verursachen. Statt der eingebauten Lastenverteilungen kann auch Drittanbieter-Software zur Lastenverteilung eingesetzt werden.

GravityZone wird als virtueller Container zur Verfügung gestellt und kann in jede virtuelle Umgebung importiert werden, egal ob sie mit VMware, Citrix oder Microsoft Hyper-V betrieben wird.

Die Integration mit VMware vCenter, Citrix XenServer und Microsoft Active Directory macht es leichter, physische und virtuelle Endpunkte gleichzeitig zu schützen.

GravityZone besteht aus den folgenden Komponenten:

- GravityZone-Virtual-Appliance
- Datenbank
- Update -Server
- Kommunikations-Server
- Web-Konsole (Control Center)
- Security Server
- Sicherheitsagenten

1.2.1. GravityZone-Virtual-Appliance

Wird GravityZone direkt im Unternehmensnetzwerk installiert, wird sie als selbst-konfigurierende virtuelle Hochsicherheits-Linux-Ubuntu-Appliance zur Verfügung gestellt, die in einem virtuellen Maschinen-Image eingebettet ist und unkompliziert über eine Befehlszeilenoberfläche installiert und konfiguriert werden kann. Die virtuelle Appliance steht in verschiedenen Formaten zur Verfügung, die

mit allen gängigen Virtualisierungsplattformen kompatibel sind (OVA, XVA, VHD, OVF, RAW).

1.2.2. GravityZone-Datenbank

Die zentrale Logik der GravityZone-Architektur. Bitdefender setzt eine nicht-relationale MongoDB-Datenbank ein, um Skalierung und Replikation zu erleichtern.

1.2.3. GravityZone-Update-Server

Der Update-Server übt die wichtige Funktion aus, die GravityZone und die Endpunkt-Agenten auf dem neuesten Stand zu halten, indem er die nötigen Pakete oder Installationsdateien repliziert und veröffentlicht.

1.2.4. GravityZone-Kommunikationsserver

Der Kommunikationsserver stellt das Bindeglied zwischen den Sicherheitsagenten und der Datenbank dar. Er übermittelt Richtlinien und Aufgaben an geschützte Endpunkte sowie die von Sicherheitsagenten gemeldeten Ereignisse.

1.2.5. Web-Konsole (Control Center)

Bitdefender-Sicherheitslösungen werden innerhalb der GravityZone von einer zentralen Stelle aus verwaltet: dem Control Center. Diese Web-Konsole erleichtert die Verwaltung, indem sie einen Überblick über die gesamte Sicherheitslage des Unternehmens bietet und die Steuerung aller Sicherheitsmodule für virtuelle und physische Arbeitsplatzrechner, Server und Mobilgeräte ermöglicht. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst der größten Unternehmen zu erfüllen.

Control Center lässt sich mit den bestehenden Systemverwaltungs- und Überwachungssystemen integrieren und macht es damit einfacher, nicht verwaltete Arbeitsplatzrechner, Server und Mobilgeräte automatisch zu schützen, die in Microsoft Active Directory, VMware vCenter oder Citric XenServer aufgeführt werden oder einfach im Netzwerk gefunden werden.

1.2.6. Security Server

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Agenten da ist und als Scan-Server fungiert.

Security Server gibt es in zwei Versionen, eine für jede Art von virtueller Umgebung:

- Security Server für Multi-Plattform-Umgebungen: muss auf genügend Hosts installiert sein, um die gewünschte Anzahl an virtuellen Maschinen gewährleisten zu können.
- Security Server für VMware-Umgebungen mit vShield Endpoint: muss auf jedem Host installiert sein, der geschützt werden soll.

1.2.7. Sicherheitsagenten

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die entsprechenden GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client

Bitdefender Endpoint Security Tools

GravityZone schützt physische und virtuelle Maschinen mit Bitdefender Endpoint Security Tools, einem intelligenten Sicherheitsagenten, der sich an die jeweilige Umgebung anpasst und je nach Endpunkttyp automatisch selbst konfiguriert. Bitdefender Endpoint Security Tools kann auf jeder beliebigen Maschine, egal ob virtuell oder physisch, installiert werden und bietet ein flexibles Scan-System. Das macht die Software zur idealen Wahl für gemischte Umgebungen (mit physischen, virtuellen und Cloud-Elementen).

Bitdefender Endpoint Security Tools schützt nicht nur das Dateisystem, sondern auch Microsoft-Exchange-Mail-Server.

Bitdefender Endpoint Security Tools benötigt nur eine einzige Richtlinienvorlage für physische und virtuelle Maschinen und nur ein einziges Installationskit für physische und virtuelle Umgebungen. Bitdefender Endpoint Security Tools ist auch mit physischen Linux-Endpunkten (Arbeitsplatzrechnern und Servern) kompatibel.

Scan-Engines

Die Scan-Engines werden während der Bitdefender Endpoint Security Tools-Paketerstellung automatisch festgelegt. Der Endpunkt-Agent erkennt dabei die Konfiguration der Maschine und passt die Scan-Technologie entsprechend an. Administratoren können die Scan-Engines auch manuell anpassen. Dabei können sie unter den folgenden Optionen wählen:

1. **Lokaler Scan**: für Scans, die auf lokalen Endpunkten durchgeführt werden. Der lokale Scan-Modus eignet sich für leistungsstarke Maschinen, auf denen alle Signaturen und Engines gespeichert sind.
2. **Hybrid-Scan mit leichten Engines (Public Cloud)**: mittlerer Ressourcenverbrauch; gescannt wird in der Cloud und zum Teil auch mithilfe lokaler Signaturen. Dieser Scan-Modus reduziert den Ressourcenverbrauch durch Auslagerung der Scan-Aktivität.
3. **Zentralisierter Scan in der Private Cloud**: geringer Ressourcenverbrauch; benötigt einen Security Server zum Scan. In diesem Fall werden keine Signaturen lokal gespeichert. Die Scan-Aktivität wird auf den Security Server ausgelagert.
4. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Volle Engines)**
5. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (Public Cloud mit leichten Engines)**

* Bei Scans mit zwei Engines wird, wenn die erste Engine nicht verfügbar ist, die Ausweich-Engine verwendet. Der Ressourcenverbrauch und die Netzwerknutzung hängen von der verwendeten Engine ab.

Sicherheitsmodule

Bitdefender Endpoint Security Tools enthält die folgenden Sicherheitsmodule:

- Malware-Schutz
- Active Virus Control
- Firewall
- Inhalts -Steuer.
- Gerätesteuerung
- Power -User

Malware-Schutz

Das Malware-Schutzmodul setzt Signatur-Scans und heuristische Analysen (B-HAVE) ein, um Sicherheit vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und anderen Arten bösartiger Software zu bieten.

Bitdefenders Technologie zur Erkennung von Malware umfasst die folgenden Sicherheitsschichten:

- Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der Signaturdatenbank abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen

spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden, sehr effektiv. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat

- Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt mutmaßliche Malware in einer virtuellen Umgebung aus, um die Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.

Active Virus Control

Für Bedrohungen, die selbst von der heuristische Engine nicht erkannt werden, wurde mit Active Virus Control (AVC) eine dritte Schutzebene eingerichtet.

Active Virus Control überwacht ununterbrochen die laufenden Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel das Verbergen des Prozesstyps, die Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, das Ablegen von Dateien, das Verbergen vor Anwendungen zur Prozessübersicht usw. Jedes verdächtige Verhalten steigert den Verdachtswert des Prozesses. Sobald ein Schwellenwert überschritten wird, wird ein Alarm ausgelöst.



Wichtig

Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Firewall

Die Firewall steuert den Zugriff von Anwendungen auf das Netzwerk sowie auf das Internet. Eine umfangreiche Datenbank enthält eine Liste bekannter, vertrauenswürdiger Anwendungen, denen automatisch Zugriff gewährt wird. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.



Wichtig
Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Inhalts -Steuer.

Mit dem Modul Inhaltssteuerung können Unternehmensrichtlinien für zugelassenen Datenverkehr, Internetzugriff, Datenschutz und Anwendungssteuerung durchgesetzt werden. Administratoren können Scan-Optionen und -Ausschlüsse für den Datenverkehr festlegen, den Internetzugriff auf bestimmte Zeiten beschränken, einzelne Internetkategorien oder URLs blockieren, Identitätsschutzregeln konfigurieren und Rechte für die Verwendung bestimmter Anwendungen festlegen.



Wichtig
Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausnahmen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich wie zum Beispiel USB-Sticks, Bluetooth-Geräte, CD/DVD-Player, Speichermedien und vieles mehr.



Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Power -User

Control-Center-Administratoren können über Richtlinieneinstellungen bestimmten Endpunkt-Benutzern Power-User-Rechte gewähren. Mit dem Power-User-Modul können Benutzern Administratorrechte verliehen werden, mit denen sie über die lokale Konsole Sicherheitseinstellungen anzeigen und verändern können. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.



Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Endpunktrollen

Relais-Rolle

Endpunktagenten mit der Rolle Bitdefender Endpoint Security Tools Relay fungieren als Kommunikations- Proxy- und Update-Server für andere Endpunkte im Netzwerk. Endpunkt-Agenten mit Relais-Rolle werden besonders in Unternehmen mit isolierten Netzwerken benötigt, in denen sämtlicher Datenverkehr über einen einzelnen Zugangspunkt läuft.

In Unternehmen mit großen, geographisch dezentralen Netzwerken reduzieren Relais-Agenten die benötigte Bandbreite, indem sie verhindern, dass geschützte Endpunkte und Security Server eine direkte Verbindung zur GravityZone herstellen.

Nachdem ein Bitdefender Endpoint Security Tools Relay im Netzwerk installiert wurde, können andere Endpunkte per Richtlinie so konfiguriert werden, dass sie über den Relais-Agenten mit dem Control Center kommunizieren.

Bitdefender Endpoint Security Tools Relay-Agenten haben die folgenden Funktionen:

- Alle ungeschützten Endpunkte im Netzwerk finden.
- Den Endpunkt-Agenten im lokalen Netzwerk installieren.
- Geschützte Endpunkte im Netzwerk auf dem neuesten Stand halten.
- Die Kommunikation zwischen dem Control Center und verbundenen Endpunkten gewährleisten.
- Als Proxy-Server für geschützte Endpunkte fungieren.
- Optimierung des Netzwerkverkehrs während Updates, Installationen, Scan-Vorgänge und andere ressourcenintensive Aufgaben ausgeführt werden.

Exchange-Schutz-Rolle

Bitdefender Endpoint Security Tools mit Exchange-Rolle kann auf Microsoft-Exchange-Servern installiert werden, um Exchange-Benutzer vor per E-Mail übertragenen Gefahren zu schützen.

Bitdefender Endpoint Security Tools mit Exchange-Rolle schützt sowohl den Server selbst als auch die Lösung Microsoft Exchange.

Endpoint Security for Mac

Endpoint Security for Mac ist ein leistungsstarker Virenscanner, der sämtliche Arten von Malware aufspüren und entfernen kann: Viren, Spyware, Trojaner,

Keylogger, Würmer und Adware. Das Programm ist auf Intel-basierte Macintosh-Arbeitsplatzrechner und -Laptops ausgelegt, auf denen Mac OS X ab Version 10.7 läuft.

Endpoint Security for Mac enthält nur das Malware-Schutz-Modul; die verfügbare Scan-Technologie ist **Lokaler Scan**; alle Signaturen und Engines werden lokal gespeichert.

GravityZone Mobile Client

Mit GravityZone Mobile Client lassen sich Sicherheitsrichtlinien leicht auf eine beliebige Anzahl von Android- und iOS-Geräten anwenden und diese Geräte so vor unbefugtem Zugriff, Riskware und Datendiebstahl schützen. Zu den Sicherheitsfunktionen gehören Bildschirmsperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht.

GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

2. INSTALLATIONSVORAUSSETZUNGEN

Alle GravityZone-Lösungen werden über das Control Center installiert und verwaltet.

2.1. Anforderungen für die GravityZone-Appliance

GravityZone wird als virtuelle Appliance angeboten. Die GravityZone-Appliance steht in den folgenden Formaten zur Verfügung:

- OVA (kompatibel mit VMware vSphere, View, VMware Player)
- XVA (kompatibel mit Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatibel mit Microsoft Hyper-V)
- OVF (kompatibel mit Red Hat Enterprise Virtualization)*
- OVF (kompatibel mit Oracle VM)*
- RAW (kompatibel mit Kernel-based Virtual Machine oder KVM)*

*OVF- und RAW-Pakete sind im Format tar.bz2 gepackt.

Mehr Details zur Kompatibilität von Oracle VM VirtualBox finden Sie in diesem Artikel.

Bitte wenden Sie sich an Bitdefender, falls Sie Unterstützung für weitere Formate oder Virtualisierungsplattformen wünschen.

2.1.1. Hardware-Anforderungen

Die Bereitstellung der GravityZone-Appliance setzt folgende Hardware-Konfiguration voraus:

- CPU: 4 virtuelle CPUs mit je 2 GHz
- Arbeitsspeicher: 8 GB
- 60 GB freier Speicherplatz

2.1.2. Internet-Verbindung

Die GravityZone-Appliance benötigt eine aktive Internet-Verbindung.

2.1.3. Anforderungen Control Center-Web-Konsole

Folgendes wird benötigt, um die Control Center-Web-Konsole aufzurufen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Empfohlene Bildschirmauflösung: 1280x800 oder höher.

- Der Computer, von dem aus Sie eine Verbindung herstellen, muss im Netzwerk mit dem Control Center verbunden sein.



Warnung
Control Center funktioniert in der Kompatibilitätsansicht des Internet Explorer 9+ nicht bzw. wird nicht richtig angezeigt. Es ist, als würden Sie eine nicht unterstützte Browserversion benutzen.

2.2. Voraussetzungen für den Schutz physischer und virtueller Endpunkte

2.2.1. Hardware-Anforderungen

Intel® Pentium kompatibler Prozessor

Betriebssysteme Arbeitsplatzrechner

- 1 GHz oder schneller bei Microsoft Windows XP SP3, Windows XP SP2 64 Bit und Windows 7 Enterprise (32 und 64 Bit)
- 2 GHz oder schneller bei Microsoft Windows Vista SP1 oder neuer (32 und 64 Bit), Microsoft Windows 7 (32 und 64 Bit), Microsoft Windows 7 SP1 (32 und 64 Bit), Windows 8
- 800 MHZ oder schneller bei Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded mit Service Pack 2, Microsoft Windows XP Tablet PC Edition

Betriebssysteme Server

- Minimum: 2,4 GHz Single-Core-CPU
- Empfohlen: 1,86 GHz oder schnellere Intel Xeon Multi-Core-CPU

Freier RAM

Benötigter Arbeitsspeicher bei der Installation (MB)

Betriebssystem	EINZELNE ENGINE					
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
Mac	1024	1024	k.A.	k.A.	k.A.	k.A.

Benötigter Arbeitsspeicher für die tägliche Nutzung (MB)*

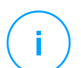
Betriebssystem	Virenschutz (einzelne Engine)			Sicherheitsmodule				
	Lokal	Hybrid	Zentrales	Verhalten Scanner	Firewall	Inhalts -Steuer.	Power -User	Update -Server
Windows	75	55	30	+13	+17	+41	+29	+76
Linux	200	180	90	-	-	-	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Festplattenanforderungen

Für die Installation benötigter freier Festplattenspeicher (MB):

Betriebssystem	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1024	1024	400	400	250	250	1024	1024	400	400
Mac	1024	1024	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.



Beachten Sie

– Für Entitäten mit der Rolle Bitdefender Endpoint Security Tools Relay werden mindestens 10 GB zusätzlicher freier Festplattenspeicher benötigt, da dort alle Updates und Installationspakete gespeichert werden.
– Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist.

Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

Standardmäßig wird der Agent auf der Systempartition installiert.

Freier Festplattenspeicher für die tägliche Nutzung (MB)*

Betriebssystem	Virenschutz (einzelne Engine)			Sicherheitsmodule				
	Lokal	Hybrid	Zentrales	Verhalten Scanner	Firewall	Inhalts -Steuer.	Power -User	Update -Server
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Bandbreitennutzung

- **Benötigte Bandbreite für Produkt-Updates zwischen dem Endpunkt-Client und dem Update-Server**

  Durch jedes regelmäßige Produkt-Update für Bitdefender Endpoint Security Tools entsteht der folgende Download-Datenverkehr an jedem Endpunkt-Client:

  – Unter Windows: ~20 MB

  – Unter Linux: ~26 MB

- **Benötigte Bandbreite für Signatur-Updates zwischen dem Endpunkt-Client und dem Update-Server**

Update-Server-Typ	Scan-Engine-Typ		
	Lokal	Hybrid	Zentrales
Relais (MB/Tag)	65	58	55
Bitdefender-Update-Server (MB/Tag)	3	3.5	3

- **Für zentralisierte Scans benötigte Bandbreite zwischen dem Endpunkt-Client und dem Security Server**

Gescannte Objekte	Art des Datenverkehrs		Download (MB)	Upload (MB)
Dateien*	Erster Scan		27	841
	Gecachter Scan		13	382
Websites**	Erster Scan	Internet-Datenverkehr	621	N/A
		Security Server	54	1050
	Gecachter Scan	Internet-Datenverkehr	654	N/A
		Security Server	0.2	0.5

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Hybrid-Scan-Datenverkehr zwischen dem Endpunkt-Client und Bitdefender Cloud Services.**

Gescannte Objekte	Art des Datenverkehrs	Download (MB)	Upload (MB)
Dateien*	Erster Scan	1.7	0.6
	Gecachter Scan	0.6	0.3
Internet-Datenverkehr**	Internet-Datenverkehr	650	N/A
	Bitdefender Cloud Services	2.6	2.7

  * Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

  ** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Datenverkehr zwischen Bitdefender Endpoint Security Tools Relay-Clients und dem Update-Server**

  Clients mit der Rolle Bitdefender Endpoint Security Tools Relay laden bei jedem unterstützten Betriebssystem ca. 700 MB / Tag vom Update-Server herunter.

- **Datenverkehr zwischen Endpunkt-Clients und dem Control Center**

  Durchschnittlich entsteht pro Tag 618 KB an Datenverkehr zwischen Endpunkt-Clients und dem Control Center.

Ressourcenverbrauch und Voraussetzungen für Systeme, die in VMware-Umgebungen mit vShield Endpoint integriert sind

Plattform	RAM	Speicherplatz
Windows	6-16* MB (~ 10 MB für die GUI)	24 MB
Linux	9-10 MB	10-11 MB

*5 MB, wenn der Hintergrund-Modus aktiviert ist, 10 MB, wenn er deaktiviert ist. Wenn der Hintergrund-Modus aktiviert ist, wird die Benutzeroberfläche von Bitdefender Endpoint Security Tools nicht automatisch beim Systemstart geladen. So werden Ressourcen freigesetzt.

2.2.2. Unterstützte Betriebssysteme

Windows-Betriebssysteme

Desktop-Betriebssysteme

- Windows 8.1*
- Windows 8**
- Windows 7
- Windows Vista mit Service Pack 1***
- Windows XP mit Service Pack 2 (64-Bit)***
- Windows XP mit Service Pack 3***

Tablets und eingebettete Betriebssysteme

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded mit Service Pack 2****
- Windows XP Tablet PC Edition****

Betriebssysteme Server:

- Windows Server 2012** / Windows Server 2012 R2*
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003 / Windows Server 2003 R2
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Small Business Server (SBS) 2003
- Windows Home Server

Beachten Sie

* VMware vShield (agentenlose Version) unterstützt Windows 8.1 (32/64-Bit) und Windows Server 2012 R2 (64-Bit) ab Vmware vSphere 5.5 – ESXi Build 1892794.
** VMware vShield (agentenlose Version) unterstützt Windows 8 und Windows Server 2012 ab VMware vShield Manager Version 5.5.
*** VMware vShield Endpoint unterstützt nicht die 64-Bit-Versionen von Windows XP und Vista.

**** Bestimmte eingebettete Betriebssystemmodule müssen installiert sein, damit Bitdefender Endpoint Security Tools funktioniert.

Linux-Betriebssysteme

- Red Hat Enterprise Linux / CentOS 5.6 oder höher
- Ubuntu 10.04 LTS oder höher
- SUSE Linux Enterprise Server 11 oder neuer
- OpenSUSE 11 oder höher
- Fedora 15 oder höher
- Debian 5.0 oder höher
- Oracle Solaris 11, 10 (nur in VMware-vShield-Umgebungen)

Zugriff-Scans sind auf allen unterstützten Gast-Betriebssystemen möglich.Auf Linux-Systemen werden Zugriff-Scans in den folgenden Fällen unterstützt:

Kernel-Version	Linux-Distribution	Zugriff-Scan-Unterstützung
2.6.38 oder höher	Alle unterstützt	Die Fanotify-Kernel-Option muss aktiviert sein.
2.6.18 - 2.6.37	Debian 5.0, 6.0 Ubuntu 10.04 LTS CentOS 6.x Red Hat Enterprise Linux 6.x	Hierfür nutzt Bitdefender DazukoFS mit vorgefertigten Kernel-Modulen.

Für andere Distributionen oder Kernel-Versionen müssen Sie das DazukoFS-Modul manuell kompilieren. Informationen zur Vorgehensweise bei der manuellen Kompilierung von DazukoFS finden Sie unter: „Unterstützung von Zugriff-Scans auf virtuellen Linux-Maschinen“ (S. 74).



Beachten Sie

Über Fanotify und DazukoFS können Anwendungen von Drittanbietern den Dateizugriff auf Linux-Systemen steuern. Weitere Informationen finden Sie unter :

- Fanotify-Manpages: http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html.
- Dazuko-Projekt-Website: http://dazuko.dnsalias.org/wiki/index.php/About.

Mac-Betriebssysteme

- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)

- Mac OS X Mavericks (10.9.x)
- Mac OS X Yosemite (10.10.x)

2.2.3. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

2.2.4. Unterstützte Virtualisierungsplattformen

Security for Virtualized Environments ist auf den folgenden Virtualisierungsplattformen sofort einsatzbereit:

- VMware vSphere 6.0, 5.5, 5.1, 5.0, 4.1 mit VMware vCenter Server 6.0, 5.5, 5.1, 5.0, 4.1
- vCNS 5.5
- VMware View 5.1, 5.0
- VMware Workstation 8.0.6, 9.x, 10.x, 11.x
- VMware Player 5.x, 6.x, 7.x
- Citrix XenServer 6.2, 6.0, 5.6 oder 5.5 (inkl. Xen Hypervisor)
- Citrix XenDesktop 7.5, 5.5 oder 5.0 (inkl. Xen Hypervisor)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 oder Windows Server 2008 R2, 2012, 2012 R2 (inkl. Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inkl. KVM Hypervisor)
- Oracle VM 3.0



Beachten Sie
Der Support oder Virtualisierungsplattformen kann auf Anfrage bereitgestellt werden.

Voraaussetzungen für die Integration mit VMware vShield Endpoint

- ESXi 5.5, 5.1, 5.0 (Version 474610 oder neuer), 4.1 (Version 433742 oder neuer)
- vCenter Server 5.5, 5.1, 5.0, 4.1
- vShield Manager 5.5, 5.1, 5.0
- vShield Endpoint, das über vShield Manager auf dem/den von Security for Virtualized Environments geschützten Host(s) installiert wurde
- VMware Tools 8.6.0 Version 446312 oder neuer, die auf den geschützten virtuellen Maschinen im vollständigen Modus oder mit dem über die VMCI im benutzerdefinierten Modus ausgewählten vShield-Endpoint-Treiber installiert wurden.



Wichtig

Es wird empfohlen, alle VMware-Produkte stets mit dem neuesten Patch auf dem neuesten Stand zu halten.

- Wenn Sie ESXi 5.5 verwenden, ist es für die Unterstützung der Gastbetriebssysteme Windows 2012 R2 und Windows 8.1 erforderlich, VMware ESXi 5.5, Patch ESXi550-201407401-BG: Updates esx-base (2077407) anzuwenden.
- Wenn Sie ESXi 5.0 verwenden, empfehlen wir dringend, VMware ESXi 5.0 Patch ESXi500-201204401-BG: Updates tools-light anzuwenden; dadurch werden kritische Probleme bei den Gast-Treibern für vShield Endpoint gelöst. Das Patch aktualisiert VMware Tools auf die Version 8.6.5-652272.
- Wenn Sie ESXi 4.1 P3 verwenden, müssen Sie sich die aktualisierte Version der VMware Tools beschaffen und sie auf den virtuellen Maschinen installieren. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

2.2.5. Unterstützte Virtualisierungs-Verwaltungs-Tools

Control Center lässt sich derzeit mit den folgenden Virtualisierungs-Verwaltungs-Tools integrieren:

- VMware vCenter Server
- Citrix XenServer

Um die Integration einzurichten, müssen Sie Benutzernamen und Passwort eines Administrators eingeben.

2.2.6. Security Server-Anforderungen

Security Server ist eine vorkonfigurierte virtuelle Maschine, die auf einem Ubuntu Server 12.04 LTS (3.2-Kernel) läuft.

Speicher- und CPU-Zuteilung für Security Server hängt von der Anzahl und Art der VMs ab, die auf dem Host laufen. In der folgenden Tabelle sind die empfohlenen Ressourcen aufgeführt:

Anzahl geschützter VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

Weitere Anforderungen hängen davon ab, ob die Appliance mit VMware vShield Endpoint integriert werden kann:

- In VMware-Umgebungen mit vShield Endpoint:
  - Security Server muss auf jedem ESXi-Host installiert werden, der geschützt werden soll.
  - Sie müssen 80 GB Speicherplatz auf jedem Host bereitstellen.
- In anderen Umgebungen:
  - Es ist zwar nicht zwingend erforderlich, aber Bitdefender empfiehlt, zur Verbesserung der Leistung Security Server auf jedem physischen Host zu installieren.
  - Sie müssen 8 GB Speicherplatz auf jedem Security Server-Host bereitstellen.

2.3. Security for Mobile-Anforderungen

2.3.1. Unterstützte Plattformen

Security for Mobile unterstützt die folgenden Mobilgeräte und Betriebssysteme:

- Apple iPhones und iPads (iOS 5.1+)
- Smartphones und Tablets mit Google Android (2.3+)

2.3.2. Verbindunugngsanforderungen

Mobile Geräte müssen eine aktive und funktionierende Funk-Daten- oder WLAN-Verbindung mit dem Kommunikationsserver haben.

2.3.3. Push-Benachrichtigungen

Security for Mobile verwendet Push-Benachrichtigungen, um Mobile Clients darauf hinzuweisen, dass Richtlinien-Updates oder Aufgaben bereit stehen. Push-Benachrichtigungen werden vom Kommunikationsserver über den Dienst gesendet, der vom Hersteller des Betriebssystems dafür vorgesehen ist:

- Google Cloud Messaging (GCM) bei Android-Geräten. Damit GCM funktioniert, müssen die folgenden Bedingungen erfüllt sein:
  - Google Play Store muss installiert sein.
  - Geräte, auf denen eine ältere Version als Android 4.0.4 läuft, müssen außerdem mindestens ein angemeldetes Google-Konto haben.
  - Um Push-Benachrichtigungen zu senden, müssen eine bestimmte Anzahl an Ports offen sein.
- Apple Push Notifications (APNs) bei iOS-Geräten. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

Mehr über die Verwaltung von mobilen Gräten mit GravityZone erfahren Sie in diesem Artikel.

2.3.4. Zertifikate für die iOS-Geräteverwaltung

Um die Infrastruktur zur Verwaltung von iOS-Mobilgeräten einzurichten, benötigen Sie bestimmte Zertifikate.

Weitere Informationen finden Sie unter „Zertifikate“ (S. 43).

2.4. Voraussetzungen für Security for Exchange

Security for Exchange wird via Bitdefender Endpoint Security Tools zur Verfügung gestellt. Die Software schützt sowohl das Dateisystem als auch den Microsoft-Exchange-Mail-Server.

2.4.1. Unterstützte Microsoft-Exchange-Umgebungen

Security for Exchange unterstützt die folgenden Microsoft-Exchange-Versionen und -Rollen:

- Exchange Server 2013 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2010 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle
- Exchange Server 2007 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle

Security for Exchange ist mit Microsoft-Exchange-Datenbankverfügbarkeitsgruppen kompatibel.

2.4.2. Systemanforderungen

Security for Exchange ist mit jedem physischen oder virtuellen 64-Bit-Server (Intel oder AMD) kompatibel, der eine unterstützte Microsoft-Exchange-Server-Version und -Rolle hat. Weitere Informationen zu Systemvoraussetzungen für Bitdefender Endpoint Security Tools finden Sie unter „Unterstützte Betriebssysteme“ (S. 17).

Empfohlene verfügbare Server-Ressourcen:

- Freier RAM: 1 GB
- Freier Festplattenspeicher: 1 GB

2.4.3. Software-Anforderungen

- Für Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 oder neuer
- Für Microsoft Exchange Server 2013 mit Service Pack 1: KB2938053 von Microsoft.

2.5. GravityZone-Kommunikations-Ports

In der folgenden Tabelle sind die Ports angegeben, die von den GravityZone-Komponenten benutzt werden:

Schnittstelle	Nutzung
80 (HTTP) / 443 (HTTPS)	Port für den Zugriff auf Control Center.
HTTP(s) 80 / 443	Bitdefender-Cloud-Spam-Erkennungsdienst
8443 (HTTPS)	Port für die Verbindung der Client/Agend-Software mit dem Kommunikationsserver.
7074 (HTTP)	Update Server Port:
7075	Sorgt für die Kommunikation zwischen GravityZone-Diensten und der Außenwelt.
4369 / 6150	Ports, die zur Sicherstellung der Kommunikation zwischen dem Control Center und dem Kommunikations-Server verwendet werden.
27017	Port, der standardmäßig vom Kommunikationsserver und Control Center zum Zugriff auf die Datenbank benutzt wird
7081 / 7083 (SSL)	Ports, die vom Endpunkt-Agenten für die Verbindung zum Security Server verwendet werden.
48651	Port zur Kommunikation zwischen dem Bitdefender Endpoint Security Tools-Agenten für Linux und Security Server in VMware-Umgebungen mit vShield Endpoint.
48652	Port zur Kommunikation zwischen dem Hypervisor (vmkernel) und Security Server in VMware-Umgebungen mit vShield Endpoint.
5228, 5229, 5230	Ports für Google Cloud Messaging (GCM). Der Kommunikationsserver benutzt GCM, um Push-Benachrichtigungen an verwaltete Android-Geräte zu senden.
2195, 2196, 5223	Ports für den Dienst Apple Push Notification (APNs). Die Ports 2195 und 2196 werden vom Kommunikationsserver dazu benutzt, mit den APNs-Servern zu kommunizieren.

Schnittstelle	Nutzung
	Port 5223 wird unter bestimmten Umständen von verwalteten iOS-Geräten benutzt, um per WLAN mit den APNs-Servern zu kommunizieren. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.
123 (UDP)	Port für User Datagram Protocol (UDP), den GravityZone-Appliances zur Zeitsynchronisation mit dem NTP-Server verwenden.
53 (UDP)	Port für Realtime Blackhole List (RBL)

Näheres zu GravityZone-Ports erfahren Sie in diesem Artikel.

3. SCHUTZ INSTALLIEREN

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren. Dazu benötigen Sie einen Control Center-Benutzer mit Administratorrechten für die Dienste, die Sie installieren möchten, und für die Netzwerk-Endpunkte, die Sie verwalten.

Die folgende Tabelle zeigt die Arten von Netzwerkobjekten, die durch die einzelnen Dienste geschützt werden:

Dienst	Netzwerkobjekte
Security for Endpoints Security for Virtualized Environments	Computer (Arbeitsplatzrechner, Laptops und Server), auf denen Microsoft Windows y Mac OS X läuft Virtuelle Maschinen, auf denen Microsoft Windows oder Linux läuft, unter einer beliebigen Virtualisierungsplattform
Security for Mobile	iPhones, iPads und Android-Geräten
Security for Exchange	Microsoft-Exchange-Server

3.1. GravityZone: Installation und Einrichtung

Führen Sie die folgenden Schritte aus, um die Installation möglichst reibungslos zu gestalten:

1. Installation vorbereiten
2. GravityZone-Virtual-Appliance installieren und einrichten
3. Verbindung zum Control Center herstellen und erstes Benutzerkonto einrichten
4. Control Center-Einstellungen konfigurieren

3.1.1. Installation vorbereiten

Zur Installation benötigen Sie ein Image der GravityZone-Virtual-Appliance. Nachdem Sie die GravityZone-Appliance installiert und eingerichtet haben, können Sie per Fernzugriff den Client installieren bzw. die nötigen Installationspakete über die Web-Oberfläche der Control Center herunterladen.

Das Image der GravityZone-Appliance steht in verschiedenen Formaten zur Verfügung, die mit den gängigsten Virtualisierungsplattformen kompatibel sind. Die Links zum Herunterladen erhalten Sie, wenn Sie sich auf den Produktseiten der Bitdefender-Enterprise-Website für eine Testversion registrieren.

Für die Installation und Ersteinrichtungen sollten Sie die folgenden Dinge zur Hand haben:

- DNS-Namen oder festgelegte IP-Adressen (entweder durch statische Konfiguration oder über DHCP-Reservierung) für die GravityZone-Appliance
- Benutzername und Passwort eines Domain-Administrators
- Eckdaten für vCenter Server, vShield Manager, XenServer (Hostname oder IP-Adresse, Kommunikations-Port, Administrator-Benutzername und -Passwort)
- Lizenzschlüssel (siehe E-Mail zur Testversions-Registrierung oder zum Kauf)
- Server-Einstellungen für ausgehende E-Mails
- wenn nötig, Proxy-Server-Einstellungen
- Sicherheitszertifikate

Zur Installation des Schutzes auf Ihren Endpunkten müssen zusätzliche Voraussetzungen erfüllt sein.

3.1.2. Die GravityZone-Appliance installieren

Die GravityZone-Appliance wird mit den folgenden vorkonfigurierten Rollen ausgeliefert:

- **Datenbank-Server**
- **Update -Server**
- **Web-Konsole**
- **Kommunikations-Server**

Gehen Sie zur Installation und Einrichtung der GravityZone-Appliance folgendermaßen vor:

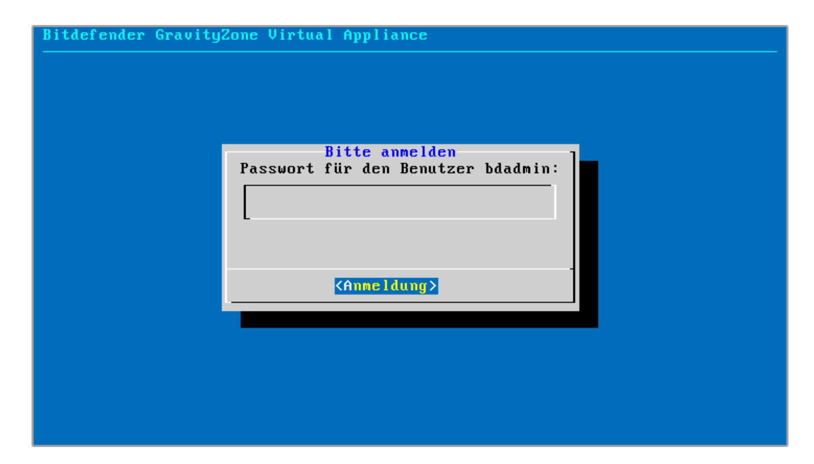
1. Importieren Sie das Image der GravityZone-Appliance in Ihre virtualisierte Umgebung.
2. Schalten Sie die Appliance an.
3. Greifen Sie von ihrem Virtualisierungsverwaltungsprogramm auf die Konsolenoberfläche der GravityZone-Appliance zu.

4. Legen Sie ein Passwort für den eingebauten Systemadministrator `bdadmin` fest.



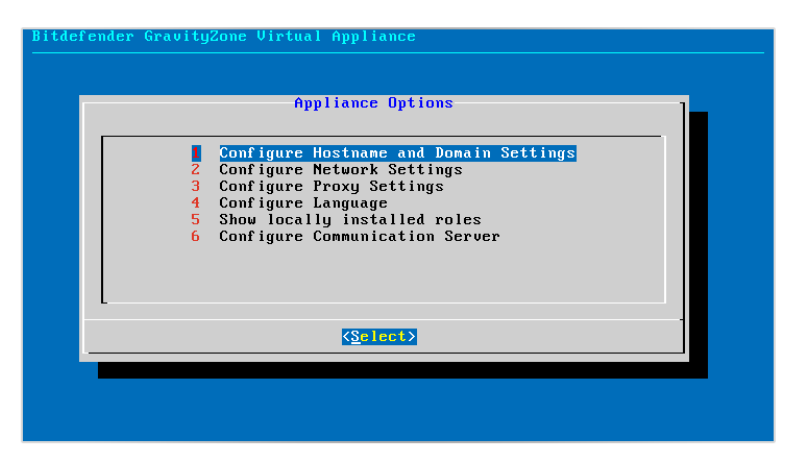
Oberfläche der Appliance-Konsole: neues Passwort eingeben

5. Melden Sie sich mit dem Passwort an, das Sie eingerichtet haben.



Konsolenoberfläche der Appliance: Login

6. Die Konfigurationsoberfläche der Appliance wird geöffnet. Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Enter`-Taste, um eine bestimmte Option auszuwählen.

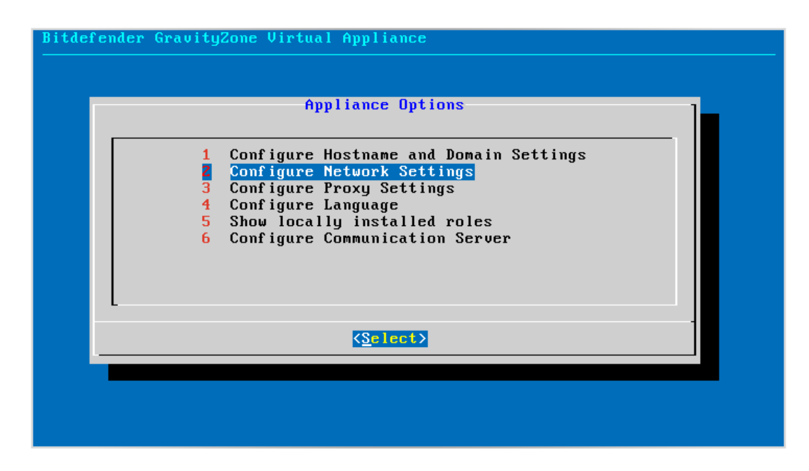


Konsolenoberfläche der Appliance: Hauptmenü

7. Konfigurieren Sie die Netzwerkeinstellungen.

   Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Wenn Sie die DHCP-Methode wählen, müssen Sie den DHCP-Server so konfigurieren, dass er eine bestimmte IP-Adresse für die Appliance reserviert.

   a. Wählen Sie aus dem Hauptmenü **Netzwerkeinstellungen konfigurieren**.

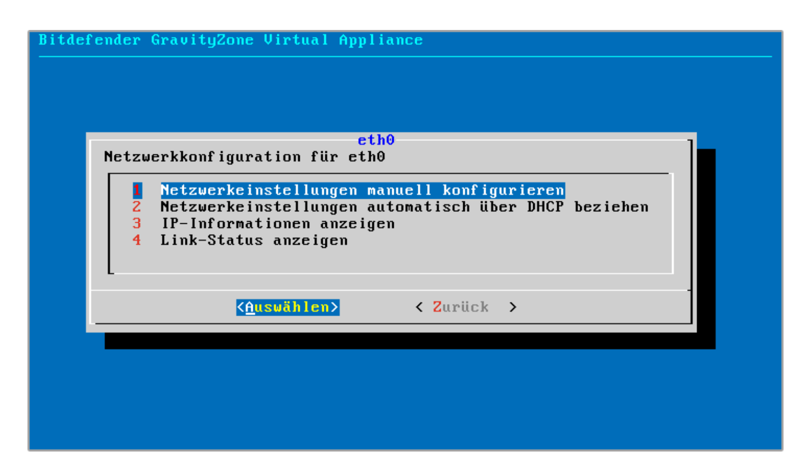


Konsolenoberfläche der Appliance: Netzwerk Einstellungoptionen

b. Wählen Sie den Netzwerkadapter aus.

c. Wählen Sie die Konfigurationsmethode:

- **Netzwerkeinstellungen manuell konfigurieren.** Sie müssen die IP-Adresse, die Netzwerkmaske, die Gateway-Adresse und die DNS-Server-Adressen angeben.
- **Netzwerkeinstellungen automatisch über DHCP beziehen.** Wählen Sie diese Option nur, wenn Sie den DHCP-Server so konfiguriert haben, dass er eine bestimmte IP-Adresse für die Appliance reserviert.



Konsolenoberfläche der Appliance: Netzwerkkonfiguration

d. Über die entsprechenden Optionen können Sie die aktuellen Details zur IP-Konfiguration bzw. den Link-Status überprüfen.

8. Konfigurieren Sie die Einstellungen für Hostnamen und Domain.

Die Kommunikation mit den GravityZone-Rollen funktioniert über die IP-Adresse oder den DNS-Namen derjenigen Appliance, auf denen die jeweilige Rolle installiert ist. Standardmäßig kommunizieren die GravityZone-Komponenten über IP-Adressen. Wenn Sie die Kommunikation über DNS-Namen ermöglichen möchten, müssen Sie der GravityZone-Appliance einen DNS-Namen zuweisen und sicherstellen, dass dieser Name korrekt zur konfigurierten IP-Adresse der Appliance aufgelöst wird.

Vorbereitende Maßnahmen:

- Konfigurieren Sie den DNS-Eintrag im DNS-Server.
- Der DNS-Name muss korrekt zur konfigurierten IP-Adresse der Appliance aufgelöst werden. Daher müssen Sie dafür sorgen, dass die Appliance die richtige IP-Adresse hat.

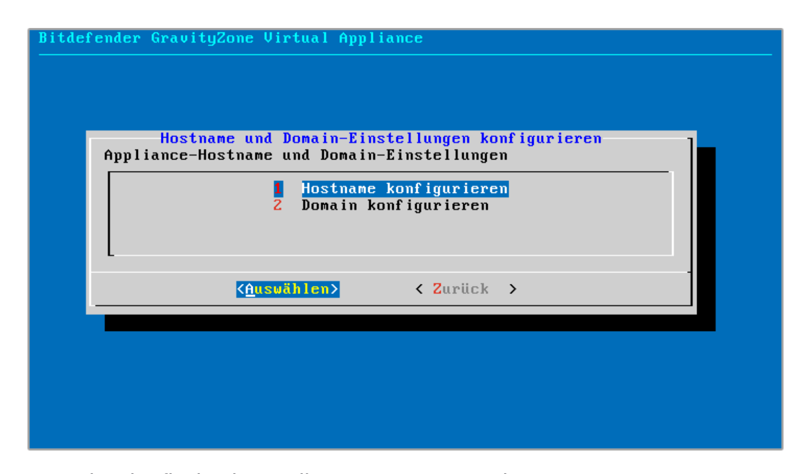
Außer der Konfiguration des Hostnamen der Appliance müssen Sie sie einer Domain zuordnen.



Wichtig
Der Hostname sollte (sofern nötig) nur während der Ersteinrichtung konfiguriert werden. Eine nachträgliche Änderungen des Hostnamen kann zu Kommunikationsfehlern mit zuvor installierten Clients führen.

So konfigurieren Sie die Einstellungen für Hostname und Domain:

a. Wählen Sie aus dem Hauptmenü **Hostname und Domain-Einstellungen konfigurieren**.



Konsolenoberfläche der Appliance: Hostname und Domänenausstattung

b. Wählen Sie **Hostname konfigurieren.**

c. Geben Sie den Hostnamen der Appliance und den Domain-Namen ein.

d. Wählen Sie **OK**, um die Änderungen zu speichern.

e. Wählen Sie **Domain konfigurieren**.

   f. Geben Sie den Benutzernamen und das Passwort eines Domain-Administrators ein.

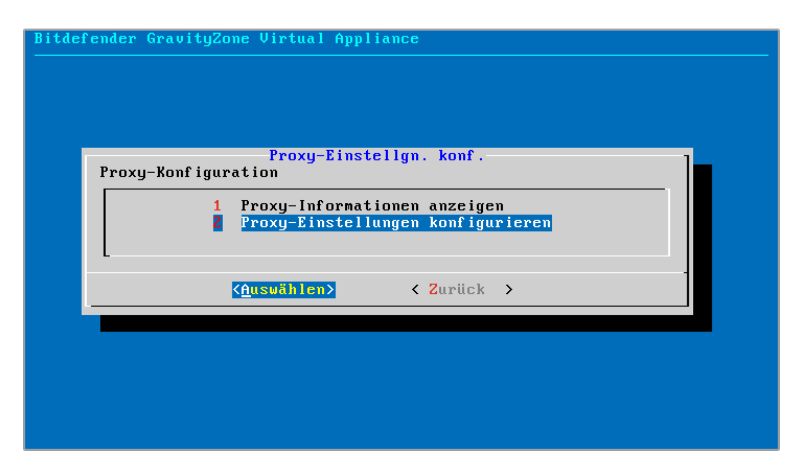
   g. Wählen Sie **OK**, um die Änderungen zu speichern.

9. Proxy-Einstellgn. konf..

   Wenn die Appliance über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren:

   a. Wählen Sie aus dem Hauptmenü **Proxy-Einstellungen konfigurieren**.

   b. Wählen Sie **Proxy-Einstellungen konfigurieren**.



Konsolenoberfläche der Appliance: Proxy-Einstellungen konfigurieren

   c. Geben Sie die Adresse des Proxy-Servers ein. Verwenden Sie die folgende Syntax:

   - Wenn der Proxy-Server keine Authentifizierung erfordert:

```
http(s)://<IP-Adresse/Hostname>:<Port>
```

   - Wenn der Proxy-Server Authentifizierung erfordert:

```
http(s)://<Benutzername>:<Passwort>@<IP-Adresse/Hostname>:<Port>
```

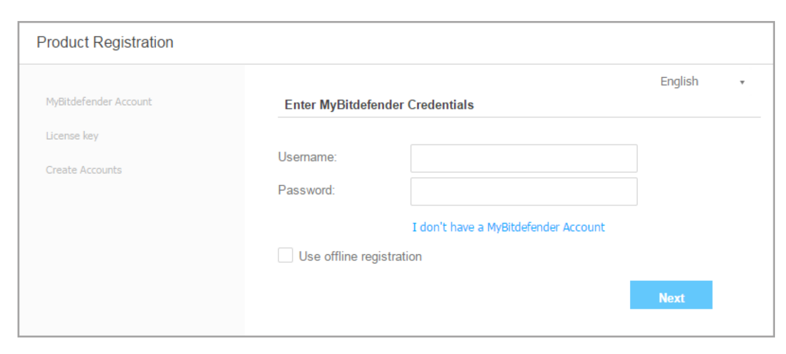
   d. Wählen Sie **OK**, um die Änderungen zu speichern.

3.1.3. Control Center: Ersteinrichtung

Nach der Installation und Einrichtung der GravityZone-Appliance müssen Sie die Web-Oberfläche des Control Center öffnen und Ihr Unternehmens-Administrator-Konto konfigurieren.

1. Geben Sie in die Adressleiste ihres Browsers IP-Adresse oder den DNS-Hostnamen der Control Center-Appliance ein (mit dem Präfix `https://`). Ein Konfigurationsassistent wird geöffnet.
2. Zunächst müssen Sie Ihre GravityZone-Installation bei einem Bitdefender-Konto registrieren. Geben Sie den Benutzernamen und das Passwort Ihres Bitdefender-Kontos ein. Wenn Sie noch kein Bitdefender-Konto haben, klicken Sie auf den entsprechenden Link, um eines zu erstellen.

   Wenn keine Internetverbindung besteht, wählen Sie **Offline-Registrierung**. In diesem Fall ist kein Bitdefender-Konto nötig.



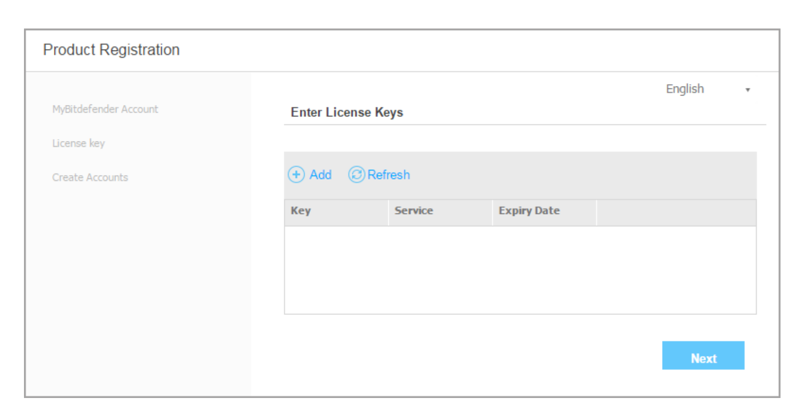
Ersteinrichtung - MyBitdefender Konto angeben

3. Klicken Sie auf **Weiter**.
4. Geben Sie den Lizenzschlüssel ein, der zur Validierung der erworbenen GravityZone-Lösung nötig ist. Sie finden Ihre Lizenzschlüssel in der E-Mail zur Testversions-Registrierung oder zum Kauf.
   a. Klicken Sie auf die Schaltfläche **Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
   b. Wählen Sie Art der Lizenzregistrierung (online oder offline).

c. Geben Sie im Feld **Lizenzschlüssel** den Lizenzschlüssel ein. Bei der Offline-Registrierung müssen Sie auch den Registrierungs-Code angeben.

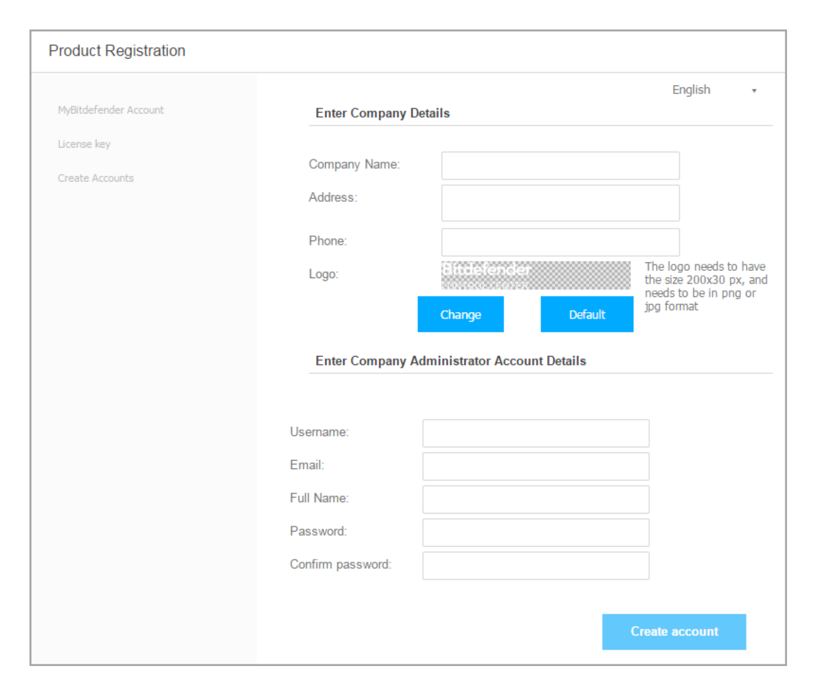
d. Warten Sie, bis der Lizenzschlüssel bestätigt wurde. Klicken Sie zum Abschluss auf **Hinzufügen**.

Der Lizenzschlüssel wird samt seinem Ablaufdatum in der Lizenztabelle angezeigt.



Ersteinrichtung - Lizenzschlüssel angeben

5. Klicken Sie auf **Weiter**.
6. Geben Sie Informationen wie den Namen, die Adresse und die Telefonnummer Ihres Unternehmens ein.
7. So können Sie das Logo, das im Control Center und in den Berichten und E-Mails Ihres Unternehmens angezeigt wird, ändern:
   - Klicken Sie auf **Ändern**, um das Logobild auf Ihrem Computer zu suchen. Das Dateiformat muss entweder PNG oder JPG sein, und das Bild muss genau 200x30 Pixel groß sein.
   - Klicken Sie auf **Standard**, um das Bild zu löschen und wieder das von Bitdefender bereitgestellte Bild zu verwenden.
8. Geben Sie die geforderten Informationen zu ihrem Unternehmens-Administrator-Konto an: Benutzername, E-Mail-Adresse und Passwort. Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten.



Ersteinrichtung - Konto konfigurieren

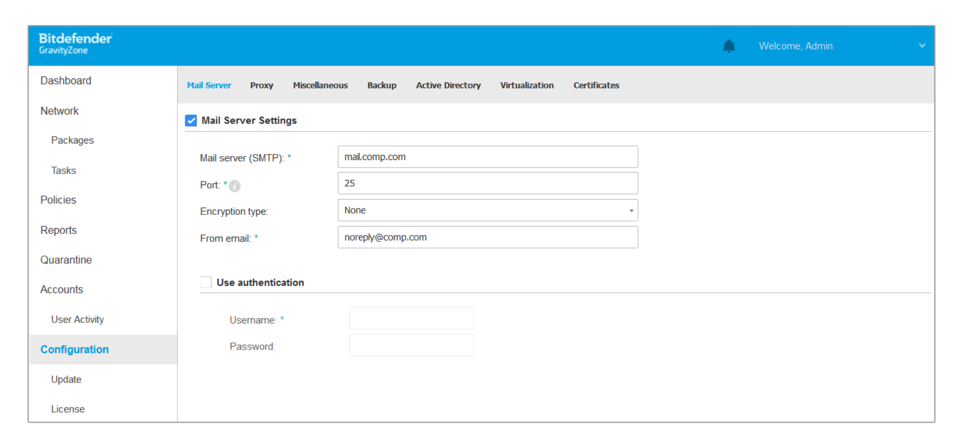
9. Klicken Sie auf **Konto erstellen**.

Das Unternehmens-Administrator-Konto wird erstellt, und Sie werden automatisch mit dem neuen Konto am Bitdefender Control Center angemeldet.

3.1.4. Control Center-Einstellungen konfig.

Nach der Ersteinrichtung müssen Sie die Einstellungen des Control Center konfigurieren. Als Unternehmensadministrator können Sie Folgendes tun:

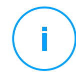
- Mail-, Proxy- und andere allgemeine Einstellungen konfigurieren.
- Ein Control Center-Datenbank-Backup durchführen oder planen.
- Integration mit Active Directory und Virtualisierungsverwaltungstools(vCenter Server, XenServer) einrichten
- Sicherheitszertifikate installieren.



Mail-Server-Einstellungen

Mail-Server

Control Center benötigt einen externen Mail-Server, um E-Mails zu versenden.



Beachten Sie

Wir empfehlen, ein eigenes Mail-Konto für Control Center zu erstellen.

So ermöglichen sie es dem Control Center E-Mails zu versenden:

1. Gehen Sie zum Seite **Konfiguration**.
2. Wechseln Sie zum Reiter **Mail-Server**.
3. Wählen Sie **Mail-Server-Einstellungen**, und konfigurieren Sie die nötigen Einstellungen:
   - **Mail-Server (SMTP).** Geben Sie die IP-Adresse oder den Host-Namen des E-Mail-Servers ein, der die E-Mails versenden wird.
   - **Schnittstelle.** Geben Sie den Port ein, über den die Verbindung zum Mail Server hergestellt werden soll.
   - **Verschlüsselungstyp.** Wenn der Mail-Server eine verschlüsselte Verbindung erfordert, wählen Sie den passenden Typ aus dem Menü (SSL,TLS oder STRARTTLS).
   - **Absender-E-Mail-Adresse.** Geben Sie die E-Mail-Adresse ein, die im Absender-Feld der E-Mail (E-Mail-Adresse des Absenders) erscheinen soll.

- **Authentifizierung verwenden.** Markieren Sie dieses Kästchen, wenn der Mail-Server eine Authentifizierung fordert. Sie müssen einen gültigen Benutzernamen/E-Mail-Adresse und ein gültiges Passwort angeben.

4. Klicken Sie auf **Speichern**.

Control Center bestätigt die Mail-Einstellungen automatisch, wenn Sie sie speichern. Wenn die angegebenen Einstellungen nicht bestätigt werden können, werden Sie durch eine Fehlermeldung auf die ungültige(n) Einstellung(en) hingewiesen. Korrigieren Sie die Einstellungen und versuchen Sie es erneut.

Proxy

Wenn Ihr Unternehmen über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren:

1. Gehen Sie zum Seite **Konfiguration**.
2. Wechseln Sie zum Reiter **Proxy**.
3. Wählen Sie **Proxy-Einstellungen verwenden**, und konfigurieren Sie die nötigen Einstellungen:
   - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
   - **Port** - Geben Sie den Port ein, über den die Verbindung zum Proxy-Server hergestellt wird.
   - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
   - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.
4. Klicken Sie auf **Speichern**.

Verschiedenes

Auf der Seite **Konfiguration** können Sie im Reiter **Verschiedenes** die folgenden Grundeinstellungen konfigurieren:

- **Gleichzeitige Installationen.** Über Installationsaufgaben können Administratoren aus der Ferne Sicherheitskomponenten installieren. Wählen Sie diese Option, um die Höchstzahl der Installationen festzulegen, die gleichzeitig vorgenommen werden können.

  Wenn die Höchstzahl der gleichzeitigen Installationen zum Beispiel auf 10 gesetzt wurde und eine Ferninstallationsaufgabe 100 Computern zugewiesen

wird, sendet Control Center zunächst 10 Installationspakete durch das Netzwerk. In diesem Fall wird die Installation gleichzeitig auf höchstens 10 Computern durchgeführt, während alle anderen Teilaufgaben zunächst den Zustand ausstehend erhalten. Sobald eine Teilaufgabe abgeschlossen ist, wird das nächste Installationspaket gesendet, usw.

- **NTP-Server-Einstellungen**. Der NTP-Server dient zur Synchronisation der Zeit mit der GravityZone-Appliance. Eine Standardadresse ist voreingestellt. Im Feld **NTP-Server-Adresse** können Sie sie ändern.



Beachten Sie
Damit die GravityZone-Appliance mit dem NTP-Server kommunizieren kann, muss Port 123 (UDP) offen sein.

- **Syslog aktivieren**. Wenn Sie diese Funktion aktivieren, erlauben Sie GravityZone, Benachrichtigungen an einen Protokollserver zu schicken, der das Syslog-Protokoll verwendet. Damit können Sie GravityZone-Ereignisse besser überwachen.

  Wie Sie die Liste der an den Syslog-Server gesendeten Benachrichtigungen anzeigen und konfigurieren können, erfahren Sie im Kapitel **Benachrichtigungen** des GravityZone-Administratorhandbuchs.

  So aktivieren Sie die Protokollierung auf einem entfernten Syslog-Server:

  1. Markieren Sie das Kästchen **Syslog aktivieren**..
  2. Geben Sie den Namen oder die IP-Adresse des Servers ein, das bevorzugte Protokoll und den Port, auf dem Syslog lauscht..
  3. Klicken Sie in der Spalte **Aktion** auf die Schaltfläche ⊕ **Hinzufügen**.

Klicken Sie **Speichern**, um die Änderungen zu speichern.

Backup

Um sicherzugehen, dass all ihre Daten im Control Center gesichert sind, sollten Sie die GravityZone-Datenbank sichern. Sie können beliebig viele Datenbank-Backups durchführen oder regelmäßige Backups zu bestimmten Zeitpunkten planen.

Mit jedem Datenbank-Backup-Befehl wird eine `tgz`-Datei (gzip-komprimierte TAR-Archivdatei) am in den erstellt.

Wenn mehrere Administratoren berechtigt sind, die Control Center-Einstellungen zu verwalten, bietet es sich an, die **Benachrichtigungseinstellungen** so zu

konfigurieren, dass Sie jedes Mal benachrichtigt werden, wenn ein Datenbank-Backup erstellt wurde. Weitere Informationen finen Sie im Kapitel **Benachrichtigungen** des GravityZone-Administratorhandbuchs.

So führen Sie ein Datenbank-Backup durch:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Backup**.
2. Klicken Sie auf die Schaltfläche **Backup jetzt durchführen** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
3. Wählen Sie die Art des Speicherorts, an dem das Backup-Archiv abgelegt wird:
   - **Lokal**, hierbei wird das Archiv auf der GravityZone-Appliance gespeichert. Dabei müssen Sie den Pfad zum Verzeichnis auf der GravityZone-Appliance angeben, in dem das Archiv gespeichert werden soll.

     Die GravityZone-Appliance hat eine Linux-Verzeichnisstruktur. Sie können das Backup-Archiv z. B. im Verzeichnis `tmp` speichern. Geben Sie dazu `/tmp` in das **Pfad**-Feld ein.
   - **FTP**, hierbei wird das Backup-Archiv auf einem FTP-Server gespeichert. Geben Sie dazu die FTP-Details in die folgenden Felder ein.
   - **Netzwerk**, hierbei wird das Archiv auf einer Netzwerkfreigabe gespeichert. Geben Sie dazu den Pfad zum gewünschten Netzwerkspeicherort ein (z. B. `\\Computer\Ordner`) sowie den Domänennamen und die Zugangsdaten des Domänenbenutzers.
4. Klicken Sie auf die Schaltfläche **Einstellungen testen**. Ein Hinweis wird Ihnen mitteilen, ob die Einstellungen gültig sind oder nicht.

   Damit das Backup erstellt werden kann müssen alle Einstellungen gültig sein.
5. Klicken Sie auf **Generieren**. Die Seite **Backup** wird geöffnet. Ein neuer Backup-Eintrag wird der Liste hinzugefügt. Überprüfen Sie den **Status** des neu erstellten Backups. Nachdem das Backup erstellt wurde, finden Sie die entsprechende `tgz`-Datei am festgelegten Speicherort.



Beachten Sie

In der Liste auf der Seite **Backup** sind die Protokolle aller erstellen Backups aufgeführt. Über die Protokolle können Sie nicht auf die Backup-Archive zugreifen; sie enthalten lediglich Informationen zu den erstellten Backups.

So planen Sie ein Datenbank-Backup:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Backup**.
2. Klicken Sie auf die Schaltfläche **Backup-Einstellungen** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
3. Wählen Sie **Geplantes Backup**.
4. Legen Sie ein Backup-Intervall (täglich, wöchentlich oder monatlich) sowie eine Startzeit fest.

   So können Sie zum Beispiel Backups wöchentlich jeden Freitag um 22:00 Uhr durchführen lassen.
5. Konfigurieren Sie den Speicherort für das Backup.
6. Wählen Sie die Art des Speicherorts, an dem das Backup-Archiv abgelegt wird:
   - **Lokal**, hierbei wird das Archiv auf der GravityZone-Appliance gespeichert. Dabei müssen Sie den Pfad zum Verzeichnis auf der GravityZone-Appliance angeben, in dem das Archiv gespeichert werden soll.

     Die GravityZone-Appliance hat eine Linux-Verzeichnisstruktur. Sie können das Backup-Archiv z. B. im Verzeichnis `tmp` speichern. Geben Sie dazu `/tmp` in das **Pfad**-Feld ein.
   - **FTP**, hierbei wird das Backup-Archiv auf einem FTP-Server gespeichert. Geben Sie dazu die FTP-Details in die folgenden Felder ein.
   - **Netzwerk**, hierbei wird das Archiv auf einer Netzwerkfreigabe gespeichert. Geben Sie dazu den Pfad zum gewünschten Netzwerkspeicherort ein (z. B. `\\Computer\Ordner`) sowie den Domänennamen und die Zugangsdaten des Domänenbenutzers.
7. Klicken Sie auf die Schaltfläche **Einstellungen testen**. Ein Hinweis wird Ihnen mitteilen, ob die Einstellungen gültig sind oder nicht.

   Damit das Backup erstellt werden kann müssen alle Einstellungen gültig sein.
8. Klicken Sie auf **Speichern**, um das geplante Backup zu erstellen.

Wie Sie ein GravityZone-Datenbank-Backup wiederherstellen, erfahren Sie in diesem Artikel.

Active Directory

Bei der Integration mit Active Directory wird das Active-Directory-Inventar in das Control Center importiert und somit die Installation, Verwaltung, Überwachung und Berichterstattung in Sachen Sicherheit vereinfacht. Active-Directory-Benutzern können im Control Center verschiedene Benutzerrollen zugewiesen werden.

So integrieren und synchronisieren Sie Control Center mit einer Active-Directory-Domain:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Active Directory**.
2. Wählen Sie **Mit Active Directory synchronisieren**, und konfigurieren Sie die nötigen Einstellungen:
   - Synchronisationsintervall (in Stunden)
   - Active-Directory-Domain-Name (inkl. Domain-Endung)
   - Benutzername und Passwort eines Domain-Administrators
3. Klicken Sie auf **Speichern**.



Wichtig
Denken Sie daran, das Benutzerpasswort auch im Control Center zu aktualisieren, wenn es sich einmal ändert.

Virtualisierung

Control Center kann derzeit mit VMware vCenter Server und Citrix XenServer integriert werden.

- „Integration mit vCenter Server“ (S. 41)
- „Integration mit XenServer“ (S. 42)



Wichtig
Vergessen Sie nicht, jedes Mal, wenn Sie eine neue Integration mit einem anderen vCenter-Server- oder XenServer-System einrichten, die Zugriffsrechte bestehender Benutzer zu überprüfen und gegebenenfalls anzupassen.

Integration mit vCenter Server

Sie können Control Center mit einem oder mehreren vCenter-Server-Systemen integrieren. vCenter Server-Systems im Linked Mode müssen separat zum Control Center hinzugefügt werden.

So richten Sie die Integration mit einem vCenter-Server ein:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Virtualisierung**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **vCenter Server** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Informationen des vCenter-Servers an.
   - Name des vCenter-Server-Systems im Control Center
   - Hostname oder IP-Adresse des vCenter-Server-Systems
   - vCenter-Server-Port (standardmäßig `443`)
4. Geben Sie die Informationen des vShield-Manager-Systems an, das mit dem vCenter-Server integriert ist (falls vorhanden).
   - Hostname oder IP-Adresse des vShield-Manager-Systems
   - vShield-Manager-Port (standardmäßig `443`)



Beachten Sie
Wenn Sie VMware vShield Endpoint in Ihrer Umgebung nicht verwenden, lassen Sie die entsprechenden Felder leer.

5. Geben Sie die Zugangsdaten für die Authentifizierung am vCenter-Server an. Sie können die Zugangsdaten für die Integration mit Active Directory oder andere Zugangsdaten verwenden. Der Benutzer, dessen Zugangsdaten Sie angeben, muss auf dem vCenter-Server Root-Administratorenrechte haben.
6. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie Netzwerkadministratoren die Berechtigung entziehen, Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht **Virtuelle Maschinen** im Netzwerkinventar ändern.
7. Klicken Sie auf **Speichern**.

Integration mit XenServer

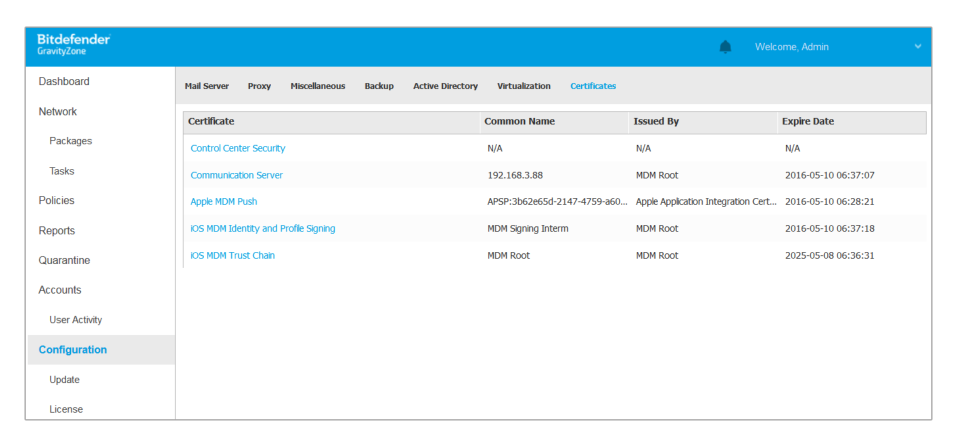
Sie können Control Center mit einem oder mehreren XenServer-Systemen integrieren.

So richten Sie die Integration mit einem XenServer ein:

1. Öffnen Sie im Control Center die Seite **Konfiguration** und klicken Sie auf den Reiter **Virtualisierung**.
2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie **XenServer** aus dem Menü. Ein Konfigurationsfenster wird sich öffnen.
3. Geben Sie die Informationen des XenServers an.
   - Name des XenServer-Systems im Control Center
   - Hostname oder IP-Adresse des XenServer-Systems
   - XenServer-Port (standardmäßig `443`)
4. Geben Sie die Zugangsdaten für die Authentifizierung am XenServer an. Sie können die Zugangsdaten für die Integration mit Active Directory oder andere Zugangsdaten verwenden.
5. **Richtlinienzuweisung aus der Netzwerkansicht einschränken**. Mit dieser Option können Sie Netzwerkadministratoren die Berechtigung entziehen, Richtlinien für virtuelle Maschinen über die Ansicht **Computer und Virtuelle Maschinen** auf der Seite **Netzwerk** zu ändern. Wenn diese Option aktiv ist, können Administratoren Richtlinien für virtuelle Maschinen nur über die Ansicht **Virtuelle Maschinen** im Netzwerkinventar ändern.
6. Klicken Sie auf **Speichern**.

Zertifikate

Damit Ihre GravityZone-Installation ordnungsgemäß funktioniert, müssen Sie eine Reihe von Sicherheitszertifikaten im Control Center erstellen und hinzufügen.



Die Seite Zertifikate

Control Center unterstützt die folgenden Zertifikatsformate:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)



Beachten Sie

Außer dem Control Center-Sicherheitszertifikat werden alle Sicherheitszertifikate ausschließlich für die Verwaltung von iOS-Geräten benötigt. Wenn Sie nicht vorhaben, iOS-Geräte zu verwalten, brauchen Sie die entsprechenden Zertifikate nicht.

Control Center-Sicherheitszertifikat

Das Sicherheitszertifikat für das Control Center wird benötigt, um die Web-Konsole des Control Center als vertrauenswürdige Website im Browser zu identifizieren. Standardmäßig verwendet Control Center ein von Bitdefender unterzeichnetes SSL-Zertifikat. Dieses eingebaute Zertifikat wird von Browsern nicht erkannt und löst Sicherheitswarnungen aus. Sicherheitswarnungen Ihres Browsers können Sie verhindern, indem Sie ein SSL-Zertifikat hinzufügen, das entweder von Ihrem Unternehmen oder von einer externen Zertifizierungsstelle (CA) unterzeichnet ist.

So fügen Sie das Control Center-Zertifikat hinzu oder ersetzen es:

1. Gehen Sie zur Seite **Konfiguration** und klicken Sie dann auf den Reiter **Zertifikate**.

2. Klicken Sie auf den Zertifikatsnamen.
3. Wählen Sie den Zertifikatstyp (mit separatem oder eingebetteten privatem Schlüssel).
4. Klicken Sie auf die Schaltfläche **Hinzufügen** neben dem Feld **Zertifikat**, und laden Sie das Zertifikat hoch.
5. Klicken Sie bei Zertifikaten mit separatem privatem Schlüssel auf die Schaltfläche **Hinzufügen** neben dem Feld **Privater Schlüssel**, und laden Sie den privaten Schlüssel hoch.
6. Wenn das Zertifikat passwortgeschützt ist, geben Sie das Passwort in das entsprechende Feld ein.
7. Klicken Sie auf **Speichern**.

3.1.5. Die GravityZone-Appliance verwalten

Die GravityZone-Appliance verfügt über eine einfache Konfigurationsoberfläche, auf die Sie von dem Verwaltungstool aus zugreifen können, mit dem Sie die virtualisierte Umgebung verwalten, in der Sie die Appliance installiert haben.

Die folgenden Optionen sind verfügbar:

- Hostname und Domäneneinstellungen konfigurieren
- Netzwerkeinstellungen konfigurieren
- Proxy-Einstellgn. konf.
- Sprache konfigurieren
- Lokal installierte Rollen anzeigen
- Kommunikationsserver konfigurieren

Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Enter`-Taste, um eine bestimmte Option auszuwählen.

Hostname und Domäneneinstellungen konfigurieren

Die Kommunikation mit den GravityZone-Rollen funktioniert über die IP-Adresse oder den DNS-Namen derjenigen Appliance, auf denen die jeweilige Rolle installiert ist. Standardmäßig kommunizieren die GravityZone-Komponenten über IP-Adressen. Wenn Sie die Kommunikation über DNS-Namen ermöglichen möchten, müssen Sie

den GravityZone-Appliances DNS-Namen zuweisen und sicherstellen, dass diese Namen korrekt zu den konfigurierten IP-Adressen der Appliances aufgelöst werden.

Vorbereitende Maßnahmen:

- Konfigurieren Sie den DNS-Eintrag im DNS-Server.
- Der DNS-Name muss korrekt zur konfigurierten IP-Adresse der Appliance aufgelöst werden. Daher müssen Sie dafür sorgen, dass die Appliance die richtige IP-Adresse hat.

Außer der Konfiguration des Hostnamen der Appliance müssen Sie sie einer Domain zuordnen.



Wichtig

Der Hostname sollte (sofern nötig) nur während der Ersteinrichtung konfiguriert werden. Eine nachträgliche Änderungen des Hostnamen kann zu Kommunikationsfehlern mit zuvor installierten Clients führen.

So konfigurieren Sie die Einstellungen für Hostname und Domain:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Hostname und Domain-Einstellungen konfigurieren**.
3. Wählen Sie **Hostname konfigurieren**.
4. Geben Sie den Hostnamen der Appliance und den Domain-Namen ein.
5. Wählen Sie **OK**, um die Änderungen zu speichern.
6. Wählen Sie **Domain konfigurieren**.
7. Geben Sie den Benutzernamen und das Passwort eines Domain-Administrators ein.
8. Wählen Sie **OK**, um die Änderungen zu speichern.

Netzwerkeinstellungen konfigurieren

Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Wenn Sie die DHCP-Methode wählen, müssen Sie den DHCP-Server so konfigurieren, dass er eine bestimmte IP-Adresse für die Appliance reserviert.

So konfigurieren Sie die Netzwerkeinstellungen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Netzwerkeinstellungen konfigurieren**.
3. Wählen Sie den Netzwerkadapter (standardmäßig `eth0`).
4. Wählen Sie die Konfigurationsmethode:
   - **Netzwerkeinstellungen manuell konfigurieren.** Sie müssen die IP-Adresse, die Netzwerkmaske, die Gateway-Adresse und die DNS-Server-Adressen angeben.
   - **Netzwerkeinstellungen automatisch über DHCP beziehen.** Wählen Sie diese Option nur, wenn Sie den DHCP-Server so konfiguriert haben, dass er eine bestimmte IP-Adresse für die Appliance reserviert.
5. Über die entsprechenden Optionen können Sie die aktuellen Details zur IP-Konfiguration bzw. den Link-Status überprüfen.

Proxy-Einstellgn. konf.

Wenn die Appliance über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren.



Beachten Sie

Die Proxy-Einstellungen können auch über das Control Center auf der Seite **Konfiguration > Proxy** konfiguriert werden. Werden die Proxy-Einstellungen an einer Stelle geändert, werden sie automatisch auch an der anderen Stelle aktualisiert.

So konfigurieren Sie die Proxy-Einstellungen:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Proxy-Einstellungen konfigurieren**.
3. Wählen Sie **Proxy-Einstellungen konfigurieren**.
4. Geben Sie die Adresse des Proxy-Servers ein. Verwenden Sie die folgende Syntax:
   - Wenn der Proxy-Server keine Authentifizierung erfordert:

     ```
     http(s)://<IP-Adresse/Hostname>:<Port>
     ```

- Wenn der Proxy-Server Authentifizierung erfordert:

  `http(s)://<Benutzername>:<Passwort>@<IP-Adresse/Hostname>:<Port>`

5. Wählen Sie **OK**, um die Änderungen zu speichern.

Sprache konfigurieren

So ändern Sie die Sprache der Befehlszeilenoberfläche:

1. Wählen Sie **Sprache konfigurieren** aus dem Hauptmenü.
2. Wählen Sie eine Sprache. Eine Bestätigungsmeldung wird angezeigt.
3. Wählen Sie **OK**, um die Änderungen zu speichern.

Lokal installierte Rollen anzeigen

Lokal installierte Rollen anzeigen

Kommunikationsserver konfigurieren



Beachten Sie
Dieser Schritt ist nur für die Verwaltung mobiler Geräte erforderlich und nur nach der Ersteinrichtung der GravityZone-Appliance verfügbar.

In der Standardeinrichtung von GravityZone können mobile Geräte nur verwaltet werden, wenn sie direkt mit dem Unternehmensnetzwerk verbunden sind (über WLAN oder VPN). Der Grund dafür ist, dass mobile Geräte bei der Registrierungen so konfiguriert werden, dass sie eine Verbindung zur lokalen Adresse der Kommunikationsserver-Appliance herstellen.

Um mobile Geräte an einem beliebigen Ort über das Internet zu verwalten, müssen Sie eine öffentlich erreichbare Adresse für den Kommunikationsserver konfigurieren.

Zur Verwaltung mobiler Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Port-Weiterleitung im Unternehmens-Gateway für die Appliance konfigurieren, auf der die Kommunikationsserver-Rolle läuft.
- Einen zusätzlichen Netzwerkadapter zur Appliance, auf der die Kommunikationsserver-Rolle läuft, hinzufügen und ihm eine öffentliche IP-Adresse zuweisen.

In beiden Fällen müssen Sie für den Kommunikationsserver die externe Adresse konfigurieren, die für die Verwaltung mobiler Geräte benutzt werden soll:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Kommunikationsserver konfigurieren**.
3. Wählen Sie **Externe Adresse des MDM-Servers konfigurieren**
4. Geben Sie die externe Adresse ein.

   Verwenden Sie die folgende Syntax: `https://<IP/Domain>:<Port>`.

   - Wenn Sie Port-Weiterleitung verwenden, müssen Sie erstens die öffentliche IP-Adresse oder den Domain-Namen und zweitens den auf dem Gateway offenen Port eingeben.
   - Wenn Sie die öffentliche Adresse des Kommunikationsservers verwenden, müssen Sie erstens die öffentliche IP-Adresse oder oder den Domain-Namen und zweitens den Kommunikationsserver-Port angeben. Der Standard-Port ist `8443`.
5. Wählen Sie **OK**, um die Änderungen zu speichern.

3.1.6. GravityZone aktualisieren

GravityZone beinhaltet eine Update-Server-Rolle, die als zentrale Update-Verteilerstation für Ihre GravityZone-Installation dient. Der Update-Server sucht nach neuen GravityZone-Updates und lädt sie von den Bitdefender-Update-Servern im Internet herunter, wonach sie lokal im Netzwerk zur Verfügung stehen. Die GravityZone-Komponenten können so konfiguriert werden, dass sie automatisch Updates vom lokalen Update-Server, und nicht aus dem Internet beziehen.

Die GravityZone-Appliance aktualisieren

Melden Sie sich zur Aktualisierung der GravityZone-Appliance und der Installationspakete der GravityZone-Komponenten mit einem Unternehmensadministratorkonto an, öffnen Sie die Seite **Update** und klicken Sie auf den Reiter **Produkt-Update**.

Vor jedem Update sollten Sie das Änderungsprotokoll der neuen Version lesen. Versionshinweise für jede neue Produktversion werden auch im Bitdefender-Support-Center veröffentlicht.

Informationen zur Version Ihrer GravityZone-Installation sowie verfügbare Updates finden Sie unter **GravityZone-Update**. Wenn ein Update verfügbar ist, können Sie auf **Jetzt aktualisieren** klicken, um die GravityZone-Appliance auf die neuste Version zu aktualisieren. Das Update kann eine kleine Weile dauern. Denken Sie daran, nach dem Update den Browser-Cache zu leeren.

Informationen zu bestehenden GravityZone-Komponentenpaketen finden Sie unter **Komponenten**. Angezeigt werden Informationen wie aktuelle Version, Update-Version (sofern zutreffend) und der Status von Update-Vorgängen, die Sie gestartet haben.

So aktualisieren Sie eine GravityZone-Komponente:

1. Markieren Sie das Kästchen für die Komponente, die Sie aktualisieren möchten.
2. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle. Die ausgewählte Komponente wird heruntergeladen/aktualisiert. Laden Sie den Tabelleninhalt neu, indem Sie auf die Schaltfläche **Neu laden** klicken. Überprüfen Sie anschließend den entsprechenden Status.



Wichtig

Standardmäßig enthält die GravityZone-Appliance nicht die Security Server-Pakete. Sie müssen die für Ihre Umgebung nötigen Security Server-Pakete manuell herunterladen.

Update-Server konfigurieren

Standardmäßig lädt der Update-Server stündlich Updates aus dem Internet. Wir empfehlen, die Standard-Update-Server-Einstellungen nicht zu verändern.

So überprüfen und konfigurieren Sie die Update-Server-Einstellungen:

1. Öffnen Sie im Control Center die Seite **Update** und klicken Sie auf den Reiter **Update-Server**.
2. Unter **Konfiguration** können Sie die wesentlichen Einstellungen überprüfen und konfigurieren.
   - **Adresse.** Der Update Server ist so eingerichtet, dass er auf `upgrade.bitdefender.com:80` nach Updates sucht und sie von dort herunterlädt. Dies ist eine generische Adresse, die Sie automatisch zu dem nächsten Server Ihrer Region weiterleitet, der Bitdefender-Updates gespeichert hat.
   - **Lokales Verzeichnis.** Updates werden in den Ordner `/opt/BitDefender/var/www` auf der GravityZone-Appliance heruntergeladen, auf der die Update Server-Rolle läuft.

- **Schnittstelle.** Der Standard-Port ist `7074`. Diesen Port müssen Sie angeben, wenn Sie die verschiedenen GravityZone-Komponenten so konfigurieren, dass sie Updates vom Update-Server beziehen.
- **Update-Intervall (Stunden).** Wenn Sie den Update-Zeitraum ändern möchten, geben Sie in diesem Feld einen neuen Wert ein.

3. Unter **Erweiterte Einstellungen** können Sie die Gateway-Rollen konfigurieren. Update Server kann als Gateway für Daten dienen, die von im Netzwerk installierten Bitdefender-Client-Produkten an Bitdefender-Server gesendet werden. Diese Daten können anonyme Berichte über Virusaktivität und Produktabstürze sowie Daten für die Online-Registrierung enthalten. Die Gateway-Rollen zu aktivieren, ist zur Steuerung des Datenverkehrs und bei Netzwerken ohne Internetzugang sinnvoll.



Beachten Sie

Sie können die Produktmodule, die statistische oder Absturzdaten an die Bitdefender-Labors senden, jederzeit deaktivieren. Zur Fernsteuerung dieser Optionen auf den von Control Center verwalteten Computern und virtuellen Maschinen können Sie Richtlinien verwenden.

4. Klicken Sie auf **Speichern**.

3.2. Lizenzmanagement

GravityZone wird mit einem einzigen Schlüssel für alle Sicherheitsdienste lizenziert.

Zur Offline-Registrierung benötigen Sie auch den Offline-Registrierungs-Code, der zum Lizenzschlüssel passt.

Sie können GravityZone testen, um zu entscheiden, ob es für Ihr Unternehmen die richtige Lösung ist. Um Ihren Testzeitraum zu aktivieren, müssen Sie Ihren Testlizenzschlüssel aus der Registrierungs-E-Mail in Control Center eingeben.



Beachten Sie

Control Center wird kostenlos mit jedem GravityZone-Sicherheitsdienst mitgeliefert.

Um GravityZone nach Ablauf des Testzeitraumes weiterhin zu nutzen, müssen Sie einen Lizenzschlüssel erwerben und damit das Produkt registrieren.

Wenn Sie eine Lizenz erwerben möchten, kontaktieren Sie einen Bitdefender-Händler, oder schreiben Sie uns eine E-Mail an enterprisesales@bitdefender.com.

GravityZone-Lizenzschlüssel können auf der Seite **Lizenz** im Control Center verwaltet werden. Wenn ihr aktueller Lizenzschlüssel bald abläuft, wird in der Konsole eine Nachricht angezeigt, die Sie darauf hinweist. Einen neuen Lizenzschlüssel eingeben oder die aktuellen Lizenzinformationen einsehen können Sie auf der Seite **Lizenz**.

3.2.1. Einen Händler finden

Unsere Händler stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl einer Lizenz-Option, die Ihren Anforderungen gerecht wird.

So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

1. Gehen Sie zur Partnersuche auf der Bitdefender-Website.
2. Wählen Sie Ihr Land, um Informationen zu Bitdefender-Partnern in Ihrer Nähe anzuzeigen.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

3.2.2. Ihren Lizenzschlüssel eingeben

Die GravityZone-Lizenz Registrierung kann online oder offline durchgeführt werden. In beiden Fällen müssen Sie einen gültigen Lizenzschlüssel eingeben.

Zur Offline-Registrierung benötigen Sie auch den Offline-Registrierungs-Code, der zum Lizenzschlüssel passt.

So registrieren Sie Ihr Produkt oder ändern den aktuellen Lizenzschlüssel:

1. Melden Sie sich mit einem Unternehmensadministratorkonto an der Control Center an.
2. Gehen Sie zur Seite **Konfiguration > Lizenz**
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle.
4. Wählen Sie den Registrierungstyp:
   - **Online**. Geben Sie einen gültigen Lizenzschlüssel für den entsprechenden Sicherheitsdienst in das Feld **Lizenzschlüssel** ein. Der Lizenzschlüssel wird online überprüft.
   - **Offline**, wenn keine Internetverbindung besteht. Hierbei müssen Sie den Lizenzschlüssel und den Registrierungscode angeben.

   Wenn der Lizenzschlüssel nicht gültig ist, wird eine Fehlermeldung als Quickinfo über dem **Lizenzschlüssel**-Feld angezeigt.

5. Klicken Sie auf **Hinzufügen**. Der Lizenzschlüssel wird auf der Seite **Lizenz** hinzugefügt. Dort werden weitere Details angezeigt.



Beachten Sie
Sie können den Lizenzschlüssel nicht löschen. Sie können einen neuen Schlüssel eingeben; es kann aber nur ein Lizenzschlüssel aktiv sein. Wenn Sie einen neuen gültigen Lizenzschlüssel eingeben (zur Registrierung oder zum Upgrade des Produkts), wird der vorherige Schlüssel ungültig. Alle ungültigen Schlüssel werden nach einer kurzen Zeit automatisch von der Seite **Lizenz** entfernt.

3.2.3. Aktuelle Lizenzinformationen anzeigen

So zeigen Sie ihre Lizenzinformationen an:

1. Melden Sie sich mit einem Unternehmensadministratorkonto an der Control Center an.
2. Gehen Sie zur Seite **Konfiguration > Lizenz**
3. In der Tabelle können Sie Details zum Lizenzschlüssel einsehen.
   - Lizenzschlüssel
   - Status des Lizenzschlüssels
   - Ablaufdatum und verbleibender Lizenzzeitraum
   - Benutzeranzahl der Lizenz

3.2.4. Benutzeranzahl der Lizenz zurücksetzen

Informationen zur Benutzeranzahl Ihrer Lizenz finden Sie auf der Seite **Lizenz** in der Spalte **Nutzung**.

Wenn Sie die Informationen zur Lizenznutzung aktualisieren möchten, können Sie den entsprechenden Lizenzschlüssel markieren und auf die Schaltfläche **Zurücksetzen** am oberen Rand der Tabelle klicken.

3.3. Die Security Server-Appliance installieren

1. Mit der Virtualisierungsplattform verbinden
2. Security Server auf Hosts installieren

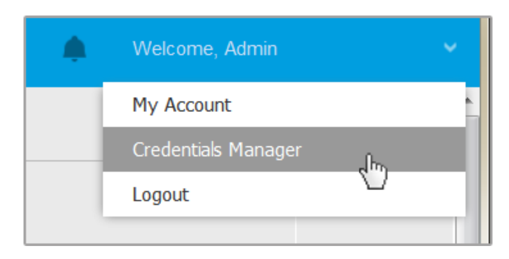
3.3.1. Mit der Virtualisierungsplattform verbinden

Um Zugriff zur mit dem Control Center integrierten virtuellen Infrastruktur zu haben, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare

Virtualisierungs-Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie in vCenter Server definiert).

So geben Sie die Zugangsdaten an, die zur Verbindung mit den Virtualisierungs-Server-Systemen nötig sind:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.



Das Netzwerk- und Pakete-Menü

2. Gehen Sie zum Reiter **Virtuelle Umgebung**.
3. Geben Sie die nötigen Authentifizierungszugangsdaten an.
   a. Wählen Sie einen Server aus dem entsprechenden Menü.



Beachten Sie
Wenn das Menü nicht verfügbar ist, wurde entweder noch keine Integration konfiguriert oder alle nötigen Zugangsdaten wurden bereits konfiguriert.

   b. Geben Sie Ihren Benutzernamen und Ihr Passwort und eine aussagekräftige Beschreibung ein.
   c. Klicken Sie auf den Button **Hinzufügen**. Die neuen Zugangsdaten werden in der Tabelle angezeigt.



Beachten Sie

Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht angegeben haben, müssen Sie sie angeben, sobald Sie das Inventar irgendeines vCenter-Server-Systems durchsuchen. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

3.3.2. Security Server auf Hosts installieren

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Clients da ist und als Scan-Server fungiert.

So installieren Sie Security Server auf Hosts:

- In VMware-Umgebungen mit vShield Endpoint müssen Sie diese spezielle Appliance auf jedem Host installieren. Alle virtuellen Maschinen auf einem Host werden automatisch über vShield Endpoint mit der Instanz von Security Server, die auf diesem Host installiert ist, verbunden.
- In allen anderen Umgebungen müssen Sie Security Server auf einem oder mehreren Hosts installieren, um die entsprechende Anzahl an virtuellen Maschinen zu schützen. Dazu müssen Sie die Anzahl der geschützten virtuellen Maschinen sowie die für Security Server auf den Hosts zur Verfügung stehenden Ressourcen und die Netzwerkverbindung zwischen Security Server und den geschützten virtuellen Maschinen bedenken. Auf virtuellen Maschinen installierte Sicherheitsagenten stellen über TCP/IP eine Verbindung zum Security Server her. Dazu verwenden sie die Informationen, die bei der Installation oder über eine Richtlinie vorgegeben werden.

Wenn Control Center mit vCenter Server und XenServer integriert ist, können Sie Security Server automatisch vom Control Center aus auf Hosts installieren. Security Server-Pakete zur Einzelinstallation können Sie auch vom Control Center herunterladen.



Beachten Sie

In VMware-Umgebungen mit vShield Endpoint können Sie Security Server nur über Installationsaufgaben auf Hosts installieren.

Lokale Installation

In allen virtualisierten Umgebungen, die nicht mit Control Center integriert sind, müssen Sie Security Server manuell mithilfe eines Installationspakets auf Hosts installieren. Das Security Server-Paket kann vom Control Center in mehreren verschiedenen Formaten heruntergeladen werden, die mit den gängigsten Virtualisierungsplattformen kompatibel sind.

Installationspakete herunterladen

So laden Sie Installationspakete für Security Server herunter:

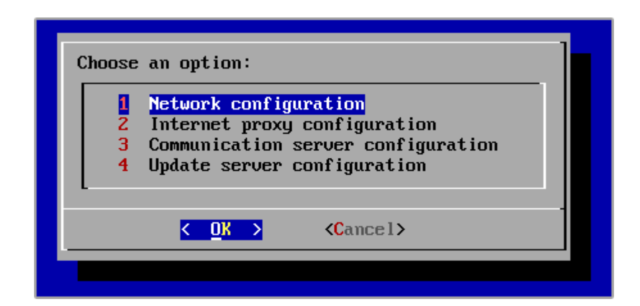
1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das Security Server-Standardpaket.
3. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Pakettyp aus dem Menü.
4. Speichern Sie das gewählte Paket am gewünschten Speicherort.

Installationspakete installieren

Sobald sie das Installationspaket haben, können Sie es auf dem Host mithilfe eines beliebigen Installationstools für virtuelle Maschinen installieren.

Richten Sie nach der Installation den Security Server wie folgt ein:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu. Alternativ können Sie auch über SSH eine Verbindung zur Appliance herstellen.
2. Melden Sie sich mit den Standardzugangsdaten an.
   - Benutzername: `root`
   - Passwort: `sve`
3. Führen Sie den Befehl `sva-setup` aus. Die Konfigurationsoberfläche der Appliance wird geöffnet.



Security Server-Konfigurationsoberfläche (Hauptmenü)

Verwenden Sie zur Navigation durch die Menüs und Optionen die `Tabulator`- und Pfeiltasten. Um eine bestimmte Option auszuwählen, drücken Sie `Enter`.

4. Konfigurieren Sie die Netzwerkeinstellungen.

Der Security Server kommuniziert mit den anderen GravityZone-Komponenten über das TCP/IP-Protokoll. Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Gehen Sie dazu wie folgt vor:

a. Wählen Sie im Hauptmenü den Punkt **Netzwerkkonfiguration**.

b. Wählen Sie den Netzwerkadapter aus.

c. Wählen Sie den IP-Adressen-Konfigurationsmodus:

- **DHCP**, wenn Sie möchten, dass der Security Server die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht.
- **Statisch**, wenn kein DHCP-Server vorhanden ist oder wenn im DHCP-Server eine IP-Adresse für die Appliance reserviert wurde. In diesem Fall müssen Sie die Netzwerkeinstellungen manuell konfigurieren.

  i. Geben Sie Hostnamen, IP-Adresse, Netzwerkmaske, Gateway und DNS-Server in die entsprechenden Felder ein.

  ii. Wählen Sie **OK**, um die Änderungen zu speichern.

Beachten Sie
Wenn Sie über einen SSH-Client mit der Appliance verbunden sind, wird Ihre Sitzung sofort beendet, wenn Sie die Netzwerkeinstellungen ändern.

5. Konfigurieren Sie die Proxy-Einstellungen.

Wenn im Netzwerk ein Proxy-Server verwendet wird, müssen Sie seine Details eingeben, damit der Security Server mit dem GravityZone Control Center kommunizieren kann.



Beachten Sie
Nur Proxy-Server mit Basic Authentication werden unterstützt.

a. Wählen Sie im Hauptmenü den Punkt **Internet-Proxy-Konfiguration**.

b. Geben Sie Hostnamen, Benutzernamen, Passwort und Domaine in die entsprechenden Felder ein.

c. Wählen Sie **OK**, um die Änderungen zu speichern.

6. Konfigurieren Sie die Adresse des Kommunikationsservers.

a. Wählen Sie im Hauptmenü den Punkt **Kommunikationsserverkonfiguration**.

b. Geben Sie die Adresse des Kommunikationsservers einschließlich der Portnummer 8443 im folgenden Format ein:

`https://Kommunikationsserver-IP-Adresse:8443`

Statt der IP-Adresse des Kommunikationsservers können Sie auch den entsprechenden Hostnamen verwenden.

c. Wählen Sie **OK**, um die Änderungen zu speichern.

7. Konfigurieren Sie die Update-Server-Adresse.
   a. Wählen Sie im Hauptmenü den Punkt **Update-Server-Konfiguration**.
   b. Standardmäßig lautet die Adresse des Update-Servers `upgrade.bitdefender.com`. Wenn Sie einen lokalen Sicherheitsagenten mit Relais-Rolle als Update-Server verwenden möchten, geben Sie seine IP-Adresse ein.
   c. Wählen Sie **OK**, um die Änderungen zu speichern.

Remote-Installation

Mit Control Center können Sie über Installationsaufgaben Security Server aus der Ferne auf sichtbaren Hosts installieren.

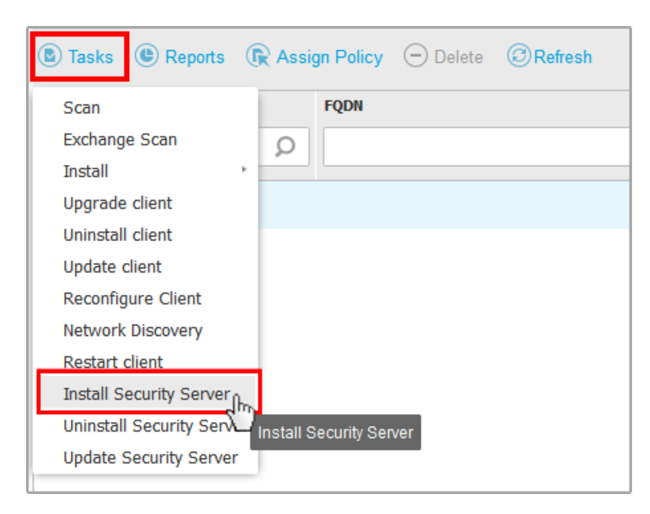
So installieren Sie Security Server aus der Ferne auf einem oder mehreren Hosts:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Durchsuchen Sie das VMware- oder Citrix-Inventar und markieren Sie die Kästchen der gewünschten Hosts oder Container (vCenter Server, XenServer oder Rechenzentrum). Um Zeit zu sparen, können Sie auch direkt den Root-Container wählen (VMware-Inventar oder Citrix-Inventar). Im Installationsassistenten können Sie Hosts einzeln auswählen.



Beachten Sie
Sie können nicht Hosts von verschiedenen Ordnern gleichzeitig auswählen.

4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle und wählen Sie **Security Server installieren** aus dem Menü. Das Fenster **Security Server-Installation** wird angezeigt.



Installieren von Security Server über das Aufgabenmenü

5. Wählen Sie den Host, auf dem Sie die Security Server-Instanzen installieren möchten.
6. Wählen Sie die gewünschten Konfigurationseinstellungen.



Wichtig

Wenn Sie bei der gleichzeitigen Installation mehrerer Instanzen von Security Server gemeinsame Einstellungen verwenden möchten, müssen die Hosts denselben Speicher benutzen, per DHCP-Server zugewiesene IP-Adressen haben und Teil desselben Netzwerks sein.

Wenn Sie jeden Security Server anders konfigurieren möchten, können Sie im nächsten Schritt des Assistenten die gewünschten Einstellungen für jeden Host einzeln vornehmen. Die folgend genannten Schritte gelten, wenn die Option **Jeden Security Server einzeln konfigurieren** verwendet wird.

7. Klicken Sie auf **Weiter**.
8. Geben Sie einen aussagekräftigen Namen für den Security Server ein.
9. Wählen Sie aus dem Menü **Container installieren** den Container, in dem Sie Security Server installieren möchten.
10. Wählen Sie den Ziel-Speicherort.

11. Wählen Sie die Art der Speicherzuweisung. Für die Installation der Appliance wird die klassische Speicherzuweisung empfohlen.



Wichtig
Wenn bei Verwendung der schlanken Speicherzuweisung der Speicherplatz knapp wird, hängt sich die Security Server auf, wodurch der Host nicht mehr geschützt ist.

12. Konfigurieren Sie die Speicher- und CPU-Ressourcenzuteilung je nach VM-Konsolidierungsrate auf dem Host. Wählen Sie **Gering**, **Mittel** oder **Hoch**, um die empfohlenen Einstellungen für die Ressourcenzuteilung zu laden, oder **Manuell**, um die Ressourcenzuteilung manuell zu konfigurieren.
13. Wenn Sie möchten, können Sie das Administratorpasswort für die Security Server-Konsole festlegen. Wenn Sie ein Administratorpasswort festlegen, setzt dieses das Standard-Root-Passwort ("sve") außer Kraft.
14. Legen Sie die Zeitzone der Appliance fest.
15. Wählen Sie die Netzwerkkonfigurationsart für das Bitdefender-Netzwerk. Die IP-Adresse des Security Server darf im Laufe der Zeit nicht geändert werden, da sie von Linux-Agenten zur Kommunikation verwendet wird.

    Wenn Sie DHCP wählen, konfigurieren Sie den DHCP-Server so, dass er eine IP-Adresse für die Appliance reserviert.

    Wenn Sie die Option "statisch" wählen, müssen Sie IP-Adresse, Subnetz-Maske, Gateway und DNS eingeben.
16. Wählen Sie das vShield-Netzwerk und geben Sie die vShield-Zugangsdaten ein. Die Standardbezeichnung für das vShield-Netzwerk `vmservice-vshield-pg`.
17. Klicken Sie auf **Speichern**.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

3.4. Bitdefender Endpoint Security Tools wird installiert ...

Um physische und virtuelle Endpunkte zu schützen, müssen Sie Bitdefender Endpoint Security Tools (die Client-Software) auf jedem Endpunkt installieren. Bitdefender Endpoint Security Tools verwaltet dann die Sicherheit auf dem jeweiligen lokalen Endpunkt. Zudem kommuniziert er mit dem Control Center, um Befehle des

Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Sie können Bitdefender Endpoint Security Tools mit den folgenden Rollen installieren:

1. Als Sicherheitsagent für Ihre Endpunkte.
2. Als Bitdefender Endpoint Security Tools Relay, und somit als Kommunikations-, Proxy- und Update-Server für andere Endpunkte im Netzwerk.

Sie können Bitdefender Endpoint Security Tools auf physischen und virtuellen Endpunkten installieren, indem Sie Installationspakete lokal ausführen oder über Control Center Installationsaufgaben aus der Ferne ausführen.

Es ist wichtig, dass Sie die Anleitung sorgfältig lesen und befolgen, um die Installation richtig vorzubereiten.

Im Normalmodus hat Bitdefender Endpoint Security Tools eine minimale Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Wenn der Netzwerkadministrator es per Installationspaket und Sicherheitsrichtlinie aktiviert hat, kann Bitdefender Endpoint Security Tools auch im Power-User-Modus ausgeführt werden. In diesem Modus kann der Endpunktbenutzer Sicherheitseinstellungen anzeigen und verändern. Der Control Center-Administrator kann jedoch in jedem Fall festlegen, welche Richtlinieneinstellungen angewendet werden und gegebenenfalls Einstellungen des Power-Users außer Kraft setzen.

Die Sprache der Benutzeroberfläche auf geschützten Endpunkten wird bei der Installation standardmäßig entsprechend der für Ihr Konto eingestellten Sprache festgelegt. Um die Benutzeroberfläche auf bestimmten Endpunkten mit einer anderen Sprache zu installieren, können Sie ein Installationspaket erstellen und die bevorzugte Sprache in den Konfigurationsoptionen dieses Pakets festlegen. Weitere Informationen zur Erstellung von Installationspaketen finden Sie unter „Installationspakete für Bitdefender Endpoint Security Tools erstellen“ (S. 63).

3.4.1. Vor der Installation

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Endpunkte die Mindestsystemanforderungen erfüllen. Bei manchen Endpunkte kann es notwendig werden, das neueste Service Pack

für das Betriebssystem zu installieren oder Speicherplatz zu schaffen. Legen Sie eine Liste der Endpunkte an, die die notwendigen Anforderungen nicht erfüllen, damit Sie diese von der Verwaltung ausschließen können.

2. Entfernen Sie alle bereits installierten Anti-Malware-, Internet-Sicherheits- und Firewall-Lösungen von den Endpunkten (eine Deaktivierung ist nicht ausreichend). Wenn Bitdefender Endpoint Security Tools gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen.

   Viele der Sicherheitsprogramme, die nicht mit Bitdefender Endpoint Security Tools kompatibel sind, werden bei der Installation automatisch erkannt und entfernt. Weitere Informationen und eine Übersicht über die Sicherheitslösungen, die erkannt werden, erhalten Sie in diesem Artikel in der Wissensdatenbank.

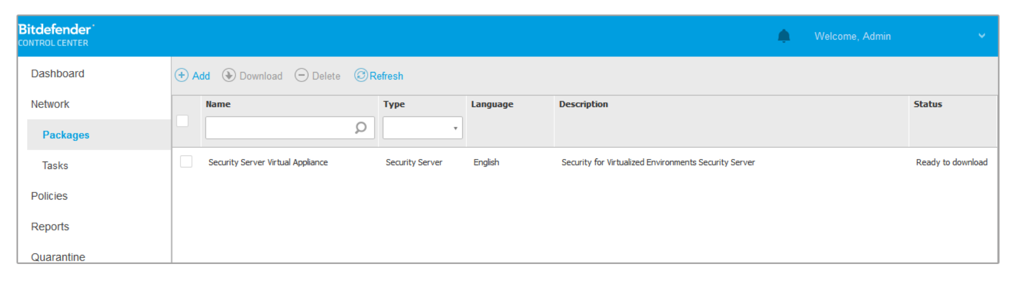
   Wichtig
   Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Sorgen Sie dafür, dass Sie alle nötigen Zugangsdaten für alle Endpunkte zur Hand haben.
4. Die Endpunkte müssen eine funktionierende Netzwerkverbindung zur Control Center-Appliance haben.

3.4.2. Lokale Installation

Eine Möglichkeit, Bitdefender Endpoint Security Tools auf einem Endpunkt zu installieren ist es, ein Installationspaket lokal auszuführen.

Sie können die Installationspakete auf der Seite **Netzwerk > Pakete** erstellen und verwalten.



Die Paketübersicht

Nach der Installation des ersten Clients wird dieser dazu verwendet, um andere Endpunkte über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu finden. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 76).

So installieren Sie Bitdefender Endpoint Security Tools lokal auf einem Endpunkt:

1. Sie können ein Installationspaket erstellen, das Ihren Anforderungen entspricht.

   Beachten Sie
   Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

2. Auf diesem Endpunkt müssen Sie zunächst das Installationspaket herunterladen.
3. Im nächsten Schritt Führen Sie das Installationspaket aus.

Installationspakete für Bitdefender Endpoint Security Tools erstellen

So erstellen Sie ein Installationspaket für Bitdefender Endpoint Security Tools:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie einen aussagekräftigen Namen und eine Beschreibung für das zu erstellende Installationspaket ein.
5. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.
6. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.



Beachten Sie
Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden.

7. Wählen Sie die Rolle des gewünschten Endpunkts:
   - **Relais**, um das Paket für einen Endpunkt mit der Rolle Bitdefender Endpoint Security Tools Relay zu erstellen. Mehr über Bitdefender Endpoint Security Tools Relay erfahren Sie unter „Relais-Rolle“ (S. 9)
   - **Exchange-Schutz**, um die Sicherheitsmodule für Microsoft-Exchange-Server zu installieren (Malware-Schutz, Spam-Schutz, Inhalts- und Anhangsfilter für den Exchange-E-Mail-Verkehr sowie Bedarf-Malware-Scans in Exchange-Datenbanken). Weitere Informationen finden Sie unter „Security for Exchange“ (S. 2).
8. **Scan-Modus**. Wählen Sie die Scan-Technologie, die am besten zu Ihrer Netzwerkumgebung und den Ressourcen Ihrer Endpunkte passt. Den Scan-Modus können Sie festlegen, indem Sie eine der folgenden Optionen wählen:
   - **Automatisch**. In diesem Fall erkennt Bitdefender Endpoint Security Tools automatisch die Konfiguration der entsprechenden Endpunkte und passt die Scan-Technologie daran an:
     – Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für physische Computer mit geringer Hardware-Leistung.
     – Lokaler Scan (mit vollen Engines) für physische Computer mit hoher Hardware-Leistung.
     – Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für virtuelle Maschinen. In diesem Fall muss mindestens ein Security Server im Netzwerk installiert sein.
   - **Benutzerdef.**. In diesem Fall können Sie für physische und virtuelle Maschinen verschiedene Scan-Technologien festlegen:
     – Zentralisierter Scan in der Private Cloud (mit Security Server)
     – Hybrid-Scan (mit leichten Engines)
     – Lokaler Scan (mit vollen Engines)

– Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (mit leichten Engines)

– Zentralisierter Scan in der Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (mit vollen Engines)

* Bei Scans mit zwei Engines wird, wenn die erste Engine nicht verfügbar ist, die Ausweich-Engine verwendet. Der Ressourcenverbrauch und die Netzwerknutzung hängen von der verwendeten Engine ab.

Weitere Informationen zu verfügbaren Scan-Technologien finden Sie hier:„Scan-Engines“ (S. 5)

9. **Endpunkt mit vShield installieren, wenn eine mit vShield integrierte VMware-Umgebung gefunden wird.** Diese Option kann gewählt werden, wenn das Installationspaket auf einer virtuellen Maschine in einer VMware-Umgebung mit vShield installiert wird. In diesem Fall wird VMware vShield Endpoint statt Bitdefender Endpoint Security Tools auf der Maschine installiert.



Wichtig
Wenn der Client auf einer virtuellen Maschine einer VMware-Umgebung mit vShield dadurch installiert wird, dass das Installationspaket lokal heruntergeladen wurde, wird Bitdefender Endpoint Security Tools anstatt VMware vShield Endpoint installiert.

10. Wenn Sie die Scan-Engines auf Private Cloud (Security Server) stellen, müssen Sie die lokal installierten Security-Server, die Sie verwenden möchten, auswählen und ihre Priorität im Bereich **Security Server-Zuweisung** konfigurieren:

- Klicken Sie auf die Liste der Security Server in der Tabellenüberschrift. Die Liste der gefundenen Security-Server wird angezeigt.
- Wählen Sie eine Entität.
- Klicken Sie in der Spaltenüberschrift **Aktionen** auf die Schaltfläche ⊕ **Hinzufügen**.

  Der Security Server wird der Liste hinzugefügt.
- Wiederholen Sie diese Schritte, wenn Sie mehrere Security-Server hinzufügen möchten, falls es mehrere gibt. In diesem Fall können Sie ihre Priorität konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile (⊙ und ⊙) klicken. Wenn der erste Security Server nicht verfügbar ist, wird der nächste verwendet, und dann der nächste, usw.

- Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⊗ **Löschen** am oberen Rand der Tabelle.

  Sie können die Verbindung zum Security Server mit der Option **SSL verwenden** verschlüsseln.

11. Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Maschinen sauber sind, bevor Sie den Client auf ihnen installieren. Es wird dann ein Cloud-Schnell-Scan auf den Maschinen ausgeführt, bevor die Installation gestartet wird.
12. Bitdefender Endpoint Security Tools wird auf den entsprechenden Endpunkten im Standardinstallationsordner installiert. Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie Bitdefender Endpoint Security Tools in einem anderen Ordner installieren möchten. Geben Sie in diesem Fall den gewünschten Pfad in das entsprechende Feld ein. Verwenden Sie dabei Windows-Konventionen (zum Beispiel `D:\Ordner`). Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.
13. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen. Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
14. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.
    - **GravityZone-Appliance**, wenn die Endpunkte eine direkte Verbindung zur GravityZone-Appliance herstellen.

      Für diesen Fall können Sie auch Folgendes definieren:

      – Einen benutzerdefinierten Kommunikationsserver; geben Sie dazu, falls erforderlich, die entsprechende IP-Adresse oder den Hostnamen ein.

      – Proxy-Einstellungen, wenn die Endpunkte über einen Proxy-Server mit der GravityZone-Appliance kommunizieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.
    - **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine.

Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.



Wichtig

Port 7074 muss offen sein, damit die Installation über einen Bitdefender Endpoint Security Tools Relay funktioniert.

15. Klicken Sie auf **Speichern**.

Das neu erstellte Paket wird zur Liste der Pakete hinzugefügt.



Beachten Sie

Die in einem Installationspaket konfigurierten Einstellungen werden sofort nach der Installation auf den jeweiligen Endpunkt angewendet. Sobald eine Richtlinie auf den Client angewendet wird, werden die Einstellungen dieser Richtlinie durchgesetzt und ersetzen gegebenenfalls die Einstellungen des Installationspakets (z. B. Kommunikationsserver oder Proxy-Einstellungen).

Installationspakete herunterladen

So laden Sie Installationspakete für Bitdefender Endpoint Security Tools herunter:

1. Melden Sie sich über den Endpunkt, auf dem Sie die Software installieren möchten, am Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Installationspaket aus, das Sie herunterladen möchten.
4. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Installer-Typ aus, den Sie verwenden möchten. Es gibt zwei Arten von Installationsdateien:
   - **Downloader**. Der Downloader lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.
   - **Installationspaket**. Die vollständigen Installationskits sind größer und sie müssen auf einem bestimmten Betriebssystem ausgeführt werden.

Das vollständige Kit ist dafür da, um den Schutz auf Endpunkten mit einer langsamen bzw. keiner Internet-Verbindung zu installieren. Laden Sie diese Datei auf einen mit dem Internet verbundenen Endpunkt herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe, um die Datei an andere Endpunkte weiterzugeben.



Beachten Sie

Verfügbare Installationspaket-Versionen:

- **Windows OS:** 32-Bit- und 64-Bit-Systeme
- **Linux OS:** 32-Bit- und 64-Bit-Systeme
- **Mac OS X:** nur 64-Bit-Systeme

Vergewissern Sie sich, dass Sie die zum jeweiligen System passende Version wählen.

5. Speichern Sie die Datei auf dem Endpunkt.



Warnung

Die Downloader-Datei darf nicht umbenannt werden, da sonst die Installationsdateien nicht vom Bitdefender-Server heruntergeladen werden können.

Installationspakete ausführen

Damit die Installation ordnungsgemäß funktioniert, muss das Installationspaket mit Administratorrechten oder unter einem Administratorkonto ausgeführt werden.

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Speichern oder kopieren Sie die Installationsdatei auf dem gewünschten Endpunkt oder auf einer Netzwerkfreigabe, auf die von dem Endpunkt aus zugegriffen werden kann.
3. Führen Sie das Installationspaket aus.
4. Folgen Sie den Instruktionen auf dem Bildschirm.

Einige Minuten nachdem Bitdefender Endpoint Security Tools installiert wurde, wird der Endpunkt im Control Center (**Netzwerk**-Seite) als verwaltet angezeigt.

3.4.3. Remote-Installation

Mit Control Center können Sie Bitdefender Endpoint Security Tools über Installationsaufgaben aus der Ferne auf Endpunkten installieren, die sich in Netzwerken befinden, die mit Control Center integriert sind, sowie auf anderen im Netzwerk gefundenen Endpunkten. In VMware-Umgebungen werden für die Ferninstallation VMware Tools benötigt, während in Citrix-XenServer-Umgebungen Windows-Administratorfreigaben SSH benötigt werden.

Nachdem Bitdefender Endpoint Security Tools auf einem Endpunkt installiert wurde, kann es einige Minuten dauern, bis die anderen Netzwerkendpunkte im Control Center angezeigt werden.

Bitdefender Endpoint Security Tools verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem Endpunkte gefunden werden können, die nicht im Active Directory sind. Die gefundenen Endpunkte werden als **nicht verwaltet** auf der **Netzwerk**-Seite angezeigt (in der Ansicht **Computer** unter **Benutzerdefinierte Gruppen**). Control Center entfernt Active-Directory-Endpunkte automatisch von der Liste der gefundenen Endpunkte.

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Endpunkt im Netzwerk installiert haben. Dieser Endpunkt wird dann verwendet, um das Netzwerk zu scannen und Bitdefender Endpoint Security Tools auf den noch nicht geschützten Endpunkten zu installieren.

Anforderungen für die Ferninstallation von Bitdefender Endpoint Security Tools

Damit die Ferninstallation funktioniert, müssen die folgenden Punkte gegeben sein:

- Auf jedem Zielendpunkt muss die Administrator-Netzwerkfreigabe admin$ aktiviert sein. Konfigurieren Sie jeden Zielarbeitsplatzrechner für die erweiterte Freigabe von Dateien.
- Schalten Sie vorübergehend die Benutzerkontensteuerung auf allen Endpunkten mit Windows-Betriebsystemen, die diese Sicherheitsfunktion beinhalten (Windows Vista, Windows 7, Windows Server 2008 etc.), aus. Wenn die Endpunkte Teil einer Domain sind, können Sie die Benutzerkontensteuerung aus der Ferne über eine Gruppenrichtlinie ausschalten.

- Deaktivieren oder beenden Sie etwaige Firewalls auf den Endpunkten. Wenn die Endpunkt Teil einer Domain sind, können Sie die Windows-Firewall aus der Ferne über eine Gruppenrichtlinie ausschalten.

So führen Sie eine Ferninstallationsaufgabe aus:

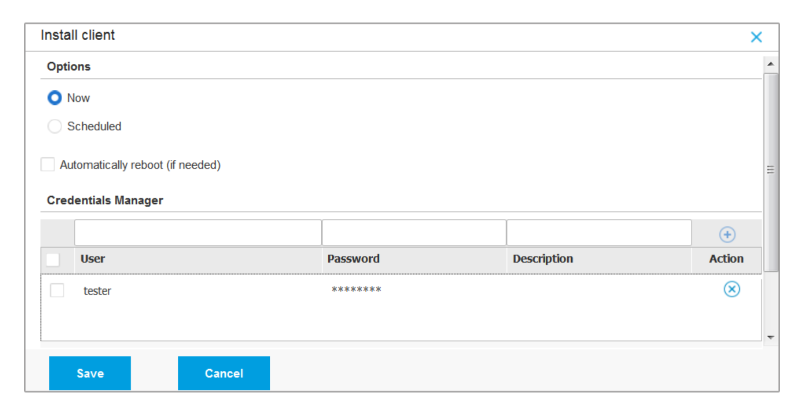
1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
4. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.



Beachten Sie
Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Endpunkte anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

5. Wählen Sie die Entitäten (Endpunkte oder Gruppen von Endpunkten) aus, auf denen Sie den Schutz installieren möchten.
6. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Installieren**.

   Der Assistent **Client installieren** wird angezeigt.



Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

7. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:
   - **Jetzt** - hiermit startet die Installation sofort.
   - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.



Beachten Sie

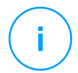
Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

8. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
9. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.



Wichtig

Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in diesem Artikel.



Beachten Sie

Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation von Bitdefender Endpoint Security Tools auf Endpunkten nicht ausgelassen werden.

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

a. Geben Sie in den entsprechenden Feldern in der Zugangsdaten-Tabellenüberschrift den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `user@domain.com` oder `domain\user`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`user@domain.com` und `domain\user`).

b. Klicken Sie auf den Button ⊕**Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.



Beachten Sie

Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben werden müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren.



Wichtig

Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

c. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.

10. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.

- **GravityZone-Appliance**, wenn die Endpunkte eine direkte Verbindung zur GravityZone-Appliance herstellen.

  Für diesen Fall können Sie auch Folgendes definieren:

  – Einen benutzerdefinierten Kommunikationsserver; geben Sie dazu, falls erforderlich, die entsprechende IP-Adresse oder den Hostnamen ein.

  – Proxy-Einstellungen, wenn die Endpunkte über einen Proxy-Server mit der GravityZone-Appliance kommunizieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.

- **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.



Wichtig
Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.



11. Im Bereich **Zusätzliche Ziele** können Sie den Client auf bestimmten Maschinen in Ihrem Netzwerk installieren, die nicht im Netzwerkinventar angezeigt werden. Vergrößern Sie den Bereich und geben Sie die IP-Adressen oder die Hostnamen dieser Maschinen, durch Kommas getrennt, in das entsprechende Feld ein. Sie können so viele IP-Adressen wie nötig hinzufügen.
12. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.
13. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

    Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Änderung von

Installationspaketen finden Sie unter „Installationspakete für Bitdefender Endpoint Security Tools erstellen“ (S. 63).

Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.

14. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

3.4.4. Unterstützung von Zugriff-Scans auf virtuellen Linux-Maschinen

Die Linux-Version von Bitdefender Endpoint Security Tools enthält die Möglichkeit Zugriff-Scans durchzuführen. Dies funktioniert auf bestimmten Linux-Distributionen und Kernel-Versionen. Bitte lesen Sie die Systemanforderungen, um zu erfahren, ob Zugriff-Scans auf Ihrer/Ihren Linux-Maschine(n) möglich sind. Im nächsten Schritt lernen Sie, wie man das DazukoFS-Modul manuell kompiliert.

Kompilieren Sie das DazukoFS-Modul manuell

Gehen Sie wie unten beschrieben vor, um DazukoFS für die Kernel-Version des Systems zu kompilieren und laden Sie danach das Modul:

1. Laden Sie die geeigneten Kernel-Header herunter.
   - Führen Sie auf **Ubuntu**-Systemen den folgenden Befehl aus:

     ```
     # sudo apt-get install linux-headers-'uname -r'
     ```

   - Führen Sie auf **RHEL/CentOS**-Systemen den folgenden Befehl aus:

     ```
     # sudo yum install kernel-devel kernel-headers
     ```

2. Auf **Ubuntu**-Systemen benötigen Sie das Paket `build-essential`:

   ```
   # sudo apt-get install build-essential
   ```

3. Kopieren und extrahieren Sie den DazukoFS-Quellcode in einem Verzeichnis Ihrer Wahl:

```
# mkdir temp
       # cd temp
       # cp /opt/BitDefender/share/src/dazukofs-source.tar.gz
       # tar -xzvf dazukofs-source.tar.gz
       # cd dazukofs-3.1.4
```

4. Kompilieren Sie das Modul:

```
# make
```

5. Installieren und laden Sie das Modul:

```
# make dazukofs_install
```

Voraussetzungen für Zugriff-Scans mit DazukoFS

Damit DazukoFS und Zugriff-Scans zusammen funktionieren, müssen die folgenden Voraussetzungen erfüllt sein. Vergewissern Sie sich das die folgenden Punkte auf Ihr Linux-System zutreffen und befolgen Sie die Anweisungen, um Probleme zu vermeiden.

- Die SELinux-Richtlinie muss deaktiviert oder auf **tolerant** gestellt sein. Sie können die Einstellungen der SELinux-Richtlinie einsehen und anpassen, indem Sie die Datei `/etc/selinux/config` bearbeiten.
- Bitdefender Endpoint Security Tools ist ausschließlich mit der Version von DazukoFS kompatibel, die im Installationspaket enthalten ist. Wenn DazukoFS auf Ihrem System bereits installiert ist, muss es vor der Installation von Bitdefender Endpoint Security Tools entfernt werden.
- DazukoFS unterstützt bestimmte Kernel-Versionen. Wenn das in Bitdefender Endpoint Security Tools enthaltene DazukoFS-Paket nicht mit der Kernel-Version des Systems kompatibel ist, kann das Modul nicht geladen werden. Ist das der Fall, können Sie den Kernel auf die unterstützte Version aktualisieren oder das DazukoFS-Modul für Ihre Kernel-Version rekompilieren. Das DazukoFS-Paket

befindet sich im Installationsverzeichnis von Bitdefender Endpoint Security Tools:

/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz

- Wenn Sie für Dateifreigaben dedizierte Server wie NFS, UNFSv3 oder Samba verwenden, müssen Sie die Dienste in der folgenden Reihenfolge starten:
  1. Aktivieren Sie im Control Center Zugriff-Scans per Richtlinie.

     Weitere Informationen hierzu finden Sie im GravityZone-Administratorhandbuch.
  2. Starten Sie den Dienst für die Netzwerkfreigabe.

     Für NFS:

     ```
     # service nfs start
     ```

     Für UNFSv3:

     ```
     # service unfs3 start
     ```

     Für Samba:

     ```
     # service smbd start
     ```



Wichtig
Beim NFS-Dienst ist DazukoFS nur mit dem NFS-User-Server kompatibel.

3.4.5. Wie die Netzwerkerkennung funktioniert

Neben der Integration mit Active Directory verfügt Security for Endpoints über automatische Netzwerkerkennungsmechanismen zur Erkennung von Arbeitsgruppen-Computern.

Security for Endpoints nutzt den **Microsoft-Computersuchdienst** für die Netzwerkerkennung. Der Computersuchdienst ist eine Netzwerktechnologie, die auf Windows-basierten Computern zum Einsatz kommt, um immer aktuelle Listen von Domänen, Arbeitsgruppen und den Computern darin zu verwalten und diese Listen bei Bedarf an Client-Computer weiterzugeben. Computer, die über den

Computersuchdienst im Netzwerk erkannt wurden, können durch Eingabe des **Net View**-Befehls im Eingabeaufforderungsfenster angezeigt werden.



Der Net-View-Befehl

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Computer im Netzwerk installiert haben. Von diesem Computer aus wird das Netzwerk gescannt.



Wichtig

Control Center bezieht keine Netzwerkinformationen über Active Directory oder über die Netzwerkübersichtsfunktion in Windows Vista und höher. Die Netzwerkübersicht nutzt eine andere Technologie zur Netzwerkerkennung: das Link-Layer-Topology-Discovery-Protokoll (LLTD).

Control Center übernimmt keine aktive Rolle bei der Ausführung des Computersuchdienstes. Bitdefender Endpoint Security Tools fragt beim Computersuchdienst lediglich die Liste der aktuell im Netzwerk sichtbaren Arbeitsplatzrechner und Server ab (die Suchliste) und leitet diese dann an das Control Center weiter. Das Control Center verarbeitet die Suchliste und fügt neu erkannte Computer zur der Liste der **nicht verwalteten Computer** hinzu. Bereits erkannte Computer werden nach einer Netzwerkerkennungsabfrage nicht gelöscht, daher müssen Computer, die sich nicht mehr länger im Netzwerk befinden, manuell ausgeschlossen und gelöscht werden.

Die erste Abfrage der Suchliste wird vom ersten im Netzwerk installierten Bitdefender Endpoint Security Tools durchgeführt.

- Falls Bitdefender Endpoint Security Tools auf einem Arbeitsgruppen-Computer installiert wurde, werden im Control Center nur die Computer dieser Arbeitsgruppe angezeigt.
- Falls Bitdefender Endpoint Security Tools auf einem Domänen-Computer installiert wurde, werden im Control Center nur die Computer dieser Domäne

angezeigt. Computer aus anderen Domänen können erkannt werden, wenn eine Vertrauensstellung mit der Domäne besteht, in der Bitdefender Endpoint Security Tools installiert ist.

Nachfolgende Netzwerkerkennungsabfragen werden danach stündlich wiederholt. Bei jeder neuen Abfrage teilt das Control Center die verwalteten Computer in Sichtbarkeitsbereiche auf und bestimmt in jedem Bereich einen Bitdefender Endpoint Security Tools zur Durchführung der Aufgabe. Ein Sichtbarkeitsbereich ist eine Gruppe von Computern, die sich gegenseitig erkennen. Normalerweise wird ein Sichtbarkeitsbereich anhand einer Arbeitsgruppe oder Domäne definiert, im Einzelfall hängt dies jedoch von der Netzwerktopologie und Konfiguration ab. Unter Umständen besteht ein Sichtbarkeitsbereich auch aus mehreren Domänen oder Arbeitsgruppen.

Falls ein ausgewähltes Bitdefender Endpoint Security Tools die Abfrage nicht durchführt, wartet Control Center auf die nächste geplante Abfrage, ohne ein anderes Bitdefender Endpoint Security Tools für einen weiteren Versuch auszuwählen.

Um das gesamte Netzwerk sichtbar zu machen, muss Bitdefender Endpoint Security Tools auf mindestens einem Computer in jeder Arbeitsgruppe oder Domäne in Ihrem Netzwerk installiert sein. Im Idealfall sollte Bitdefender Endpoint Security Tools auf mindestens einem Computer in jedem Subnetzwerk installiert sein.

Weitere Informationen zum Microsoft-Computersuchdienst

Der Computersuchdienst auf einen Blick:

- Funktioniert unabhängig von Active Directory.
- Läuft ausschließlich über IPv4-Netzwerken und funktioniert unabhängig innerhalb der Grenzen einer LAN-Gruppe (Arbeitsgruppe oder Domäne). Eine Suchliste wird für jede LAN-Gruppe erstellt und verwaltet.
- Nutzt für die Kommunikation zwischen den Knoten üblicherweise verbindungslose Server-Übertragungen.
- Nutzt NetBIOS über TCP/IP (NetBT).
- Benötigt NetBIOS-Namensauflösung. Es wird empfohlen im Netzwerk eine Windows-Internet-Name-Service-Infrastruktur (WINS) zu unterhalten.
- Ist standardmäßig nicht in Windows Server 2008 und 2008 R2 aktiviert.

Weitere Informationen zum Computersuchdienst finden Sie in der Computer Browser Service Technical Reference im Microsoft Technet.

Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über das Control Center verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein. Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein. Die lokale Firewall muss NetBT-Verkehr zulassen.
- Die Freigabe von Dateien muss auf den Computern aktiviert sein. Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.
- Für Windows Vista und höher muss die Netzwerkerkennung aktiviert werden (**Systemsteuerung > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktion aktivieren zu können, müssen zunächst die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost
- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Bitdefender Endpoint Security Tools den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.



Beachten Sie

Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.

3.5. Security for Exchange installieren

Security for Exchange integriert sich automatisch mit den Excchange-Servern je nach Server-Rolle. Für jede Rolle werden entsprechend der folgenden Übersicht nur die kompatiblen Funktionen installiert:

	Microsoft Exchange 2013		Microsoft Exchange 2010/2007		
Bestandteile	**Edge**	**Postfach**	**Edge**	**Hub**	**Postfach**
Transport-Ebene					
Antimalware Filtering	x	x	x	x	
Antispam Filtering	x	x	x	x	
Content Filtering	x	x	x	x	
Attachment Filtering	x	x	x	x	
Exchange-Informationsspeicher					
On-demand antimalware scanning		x			x

3.5.1. Vor der Installation

Bevor Sie Security for Exchange installieren, sollten Sie sich vergewissern, dass alle Voraussetzungen erfüllt sind, da sonst eventuell Bitdefender Endpoint Security Tools ohne das Exchange-Schutz-Modul installiert wird.

Damit das Exchange-Schutz-Modul möglichst reibungslos läuft und etwaige Konflikte und unerwünschte Ergebnisse vermieden werden, sollten Sie andere Malware-Schutz- und E-Mail-Filter-Agenten deinstallieren.

Bitdefender Endpoint Security Tools findet und entfernt die meisten Malware-Schutz-Produkte automatisch und deaktiviert auch den eingebauten Malware-Schutz-Agenten von Exchange Server 2013. Eine Liste aller automatisch gefundenen und entfernten Sicherheitssoftware finden Sie in diesem Artikel.

Den eingebauten Exchange-Malware-Schutz-Agenten können Sie jederzeit manuell wieder aktivieren. Dies wird jedoch nicht empfohlen.

3.5.2. Schutz auf Exchange-Servern installieren

Um Ihre Exchange-Server zu schützen, müssen Sie Bitdefender Endpoint Security Tools mit der Exchange-Schutz-Rolle auf jedem dieser Server installieren.

Dazu haben Sie verschiedene Möglichkeiten:

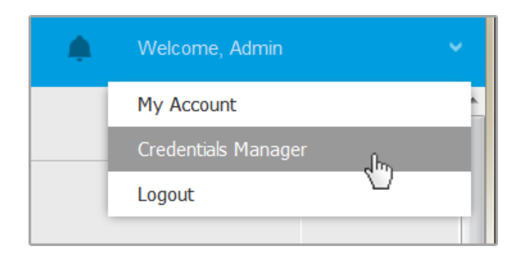
- Lokale Installation durch Herunterladen und Ausführen des Installationspakets auf dem jeweiligen Server.
- Ferninstallation durch Ausführen der Aufgabe **Installieren**.
- Per Fernzugriff durch Ausführen der Aufgabe **Client neu konfigurieren**, falls Bitdefender Endpoint Security Tools bereits das Dateisystem auf dem Server schützt.

Weitere Details zur Installation finden Sie unter „Bitdefender Endpoint Security Tools wird installiert ...“ (S. 60).

3.6. Zugangsdaten-Manager

Der Zugangsdaten-Manager hilft Ihnen dabei, die Zugangsdaten festzulegen, die zum Zugriff auf die verfügbaren vCenter-Server-Inventare sowie zur Fernauthentifizierung bei verschiedenen Betriebssystemen in Ihrem Netzwerk benötigt werden.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.



Das Zugangsdaten-Manager-Menü

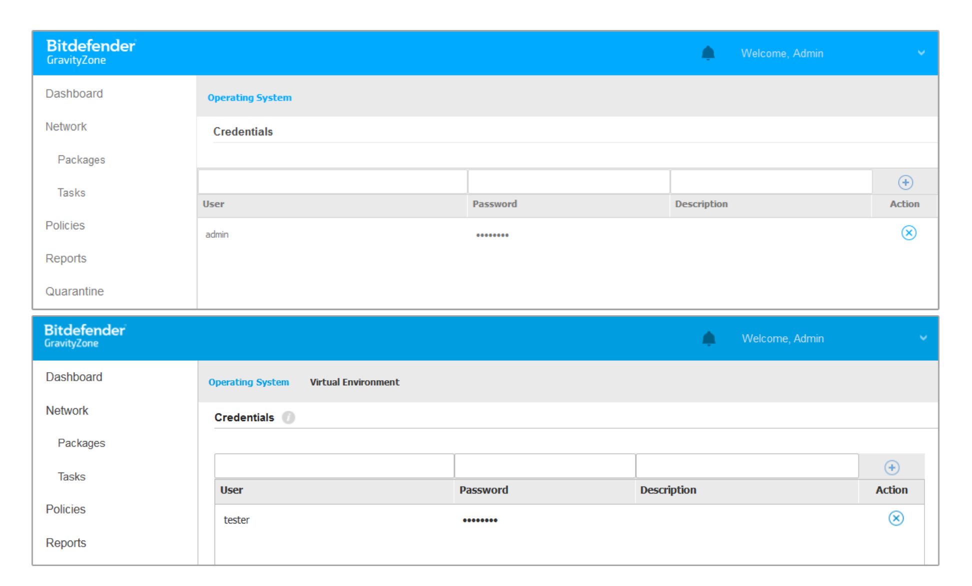
Das Fenster **Zugangsdaten-Manager** hat zwei Reiter:

- Betriebssystem
- Virtuelle Umgebung

3.6.1. Betriebssystem

Im Reiter **Betriebssystem** können Sie die Administrator-Zugangsdaten verwalten, die für die Fernauthentifizierung während der Ausführung von Installationsaufgaben auf Computern und virtuellen Maschinen in Ihrem Netzwerk nötig sind.

So fügen Sie Zugangsdaten hinzu:



Zugangsdaten-Manager

1. Geben Sie in die entsprechenden Felder im oberen Bereich der Tabelle den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `Benutzername@domain.com` oder `Domain\Benutzername`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).

2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.



Beachten Sie

Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

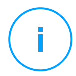
3.6.2. Virtuelle Umgebung

Im Reiter Virtuelle Umgebung können Sie die Zugangsdaten für die verfügbaren virtuellen Server-Systeme verwalten.

Um Zugriff zur mit dem Control Center integrierten virtuellen Infrastruktur zu haben, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare Virtualisierte-Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie im virtualisierten Server definiert).

So legen Sie die Zugangsdaten fest, die für die Verbindung zu einem virtualisierten Server nötig sind:

1. Wählen Sie den Server aus dem entsprechenden Menü.



Beachten Sie

Wenn das Menü nicht verfügbar ist, wurde entweder noch keine Integration konfiguriert oder alle nötigen Zugangsdaten wurden bereits konfiguriert.

2. Geben Sie Ihren Benutzernamen und Ihr Passwort und eine aussagekräftige Beschreibung ein.
3. Klicken Sie auf den Button ⊕**Hinzufügen**. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.



Beachten Sie

Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht im Zugangsdaten-Manager konfigurieren, müssen Sie sie angeben, sobald Sie das Inventar irgendeines Virtualisierte-Server-Systems durchsuchen. Wenn Sie Ihre

Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.



Wichtig

Wenn Sie Ihr Passwort für Ihren virtualisierten Server ändern, müssen Sie es auch im Zugangsdaten-Manager aktualisieren.

3.6.3. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche ⊗ **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile. Das ausgewählte Konto wird gelöscht.

3.7. Security for Mobile installieren

Security for Mobile ist eine Lösung zur Verwaltung mobiler Geräte für iPhones, iPads und Android-Geräte. Eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Systemanforderungen.

Damit Sie Security for Mobile vom Control Center aus verwalten können, müssen Sie Active-Directory-Benutzern oder benutzerdefinierten Benutzern Mobilgeräte hinzufügen und anschließend die App GravityZone Mobile Client auf den Geräten installieren. Nach der Einrichtung können Sie Verwaltungsaufgaben auf Mobilgeräten ausführen.

Bevor Sie loslegen, sollten Sie eine öffentliche (externe) Adresse für den Kommunikationsserver konfigurieren.

So installieren Sie Security for Mobile:

1. Wenn Sie die Integration mit Active Directory nicht benutzen, müssen Sie Benutzer für Eigentümer mobiler Geräte erstellen.
2. Benutzern Geräte hinzufügen.
3. GravityZone Mobile Client auf Geräten installieren und aktivieren.

3.7.1. Externe Adresse für den Kommunikationsserver konfigurieren

In der Standardeinrichtung von GravityZone können mobile Geräte nur verwaltet werden, wenn sie direkt mit dem Unternehmensnetzwerk verbunden sind (über WLAN oder VPN). Der Grund dafür ist, dass mobile Geräte bei der Registrierungen so konfiguriert werden, dass sie eine Verbindung zur lokalen Adresse der Kommunikationsserver-Appliance herstellen.

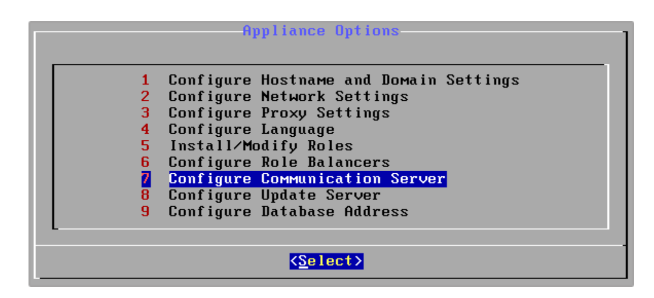
Um mobile Geräte an einem beliebigen Ort über das Internet zu verwalten, müssen Sie eine öffentlich erreichbare Adresse für den Kommunikationsserver konfigurieren.

Zur Verwaltung mobiler Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Port-Weiterleitung im Unternehmens-Gateway für die Appliance konfigurieren, auf der die Kommunikationsserver-Rolle läuft.
- Einen zusätzlichen Netzwerkadapter zur Appliance, auf der die Kommunikationsserver-Rolle läuft, hinzufügen und ihm eine öffentliche IP-Adresse zuweisen.

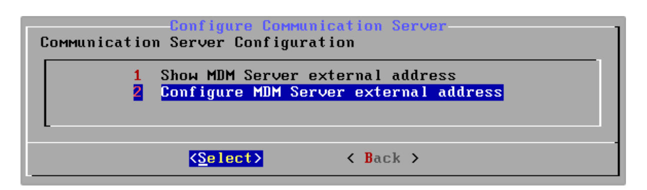
In beiden Fällen müssen Sie für den Kommunikationsserver die externe Adresse konfigurieren, die für die Verwaltung mobiler Geräte benutzt werden soll:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Kommunikationsserver konfigurieren**.



Fenster "Anwendungsoptionen"

3. Wählen Sie **Externe Adresse des MDM-Servers konfigurieren**



Fenster "Kommunikationsserver konfigurieren"

4. Geben Sie die externe Adresse ein.

   Verwenden Sie die folgende Syntax: `https://<IP/Domain>:<Port>`.



Fenster für die Eingabe der externen Adresse des MDM-Servers

- Wenn Sie Port-Weiterleitung verwenden, müssen Sie erstens die öffentliche IP-Adresse oder den Domain-Namen und zweitens den auf dem Gateway offenen Port eingeben.
- Wenn Sie die öffentliche Adresse des Kommunikationsservers verwenden, müssen Sie erstens die öffentliche IP-Adresse oder oder den Domain-Namen und zweitens den Kommunikationsserver-Port angeben. Der Standard-Port ist `8443`.

5. Wählen Sie **OK**, um die Änderungen zu speichern.

3.7.2. Benutzerdefinierte Benutzer erstellen und organisieren

In Situationen ohne Active Directory müssen Sie zunächst benutzerdefinierte Benutzer erstellen, um eine Möglichkeit zu haben, die Eigentümer von Mobilgeräten zu identifizieren.Angegebene Benutzer mobiler Geräte werden in keiner Weise mit dem Active Directory oder mit anderen im Control Center definierten Benutzern verknüpft.

Benutzerdefinierte Benutzer erstellen

So erstellen Sie einen benutzerdefinierten Benutzer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der Ansichtsauswahl.
3. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**.
4. Klicken Sie auf das Symbol **Benutzer hinzufügen** in der Symbolleiste. Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die Informationen des gewünschten Benutzers an:
   - Einen aussagekräftigen Benutzernamen (z. B. den vollen Namen des Benutzers)
   - Die E-Mail-Adresse des Benutzers



Wichtig

- Vergewissern Sie sich, dass die E-Mail-Adresse gültig ist. Wenn Sie ein Gerät hinzufügen, erhält der Benutzer eine E-Mail mit den Installationsanweisungen.
- Jede E-Mail-Adresse kann nur zu einem Benutzer gehören.

6. Klicken Sie auf **OK**.

Benutzerdefinierte Benutzer organisieren

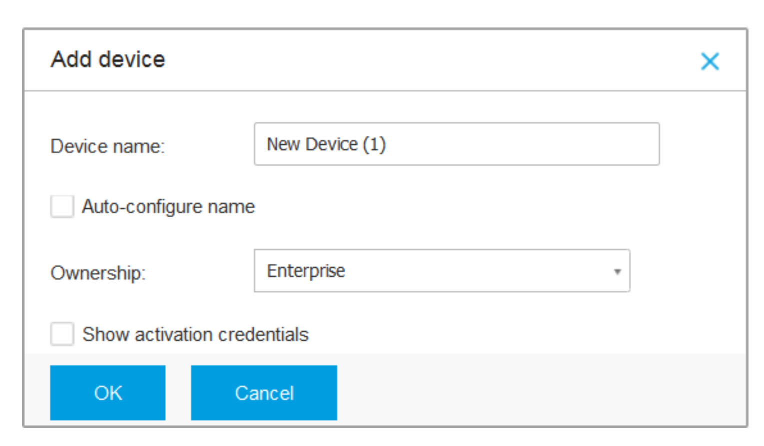
So organisieren Sie benutzerdefinierte Benutzer:

1. Erstellen Sie benutzerdefinierte Gruppen.
   a. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**, und klicken Sie auf das Symbol **Hinzufügen** in der Symbolleiste (über dem Fenster).
   b. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK** Die neue Gruppe wird jetzt unter **Benutzerdefinierte Gruppen** angezeigt.
2. Verschieben Sie benutzerdefinierte Benutzer in entsprechende benutzerdefinierte Gruppen.
   a. Wählen Sie im rechten Fenster die Benutzer.
   b. Verschieben Sie Ihre Auswahl per Drag und Drop in die gewünschte Gruppe im linken Fenster.

3.7.3. Benutzern Geräte hinzufügen

So fügen Sie einem Benutzer ein Gerät hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der Ansichtsauswahl.
3. Suchen Sie den Benutzer in den Active-Directory-Ordnern oder in benutzerdefinierten Gruppen.
4. Klicken Sie auf das Symbol ⊕ **Gerät hinzufügen** am oberen Rand der Netzwerktabelle. Ein Konfigurationsfenster wird sich öffnen.



Ein Mobilgerät für einen Benutzer hinzufügen

5. Geben Sie einen aussagekräftigen Namen für das Gerät ein.
6. Mit der Option **Name automatisch konfigurieren** wird der Gerätename automatisch generiert. Nach dem Hinzufügen erhält das Gerät einen generierten Namen. Sobald das Gerät aktiviert ist, wird es automatisch mithilfe der entsprechenden Hersteller- und Modell-Informationen umbenannt.
7. Wählen Sie den Eigentümertyp des Geräts (geschäftlich/enterprise oder privat).
8. Wählen Sie die Option **Aktivierungszugangsdaten anzeigen** aus, nachdem Sie auf **OK** geklickt haben, wenn Sie den GravityZone Mobile Client auf dem Gerät des Benutzers installieren möchten.

9. Klicken Sie auf **OK**. Es wird sofort eine E-Mail an den Benutzer gesendet, die Installationsanweisungen und Aktivierungsdetails für das Gerät enthält. Die Aktivierungsdetails enthalten das Aktivierungs-Token und die Adresse des Kommunikationsservers (und den entsprechenden QR-Code).



Beachten Sie
Sie können die Aktivierungsdetails eines Geräts jederzeit einsehen, indem Sie im Control Center auf seinen Namen klicken.



Beachten Sie
Sie können auch einer Auswahl an Benutzern und Gruppen mobile Geräte hinzufügen. In diesem Fall können Sie im Konfigurationsfenster nur die Eigentümer der Geräte definieren. Mobile Geräte, die durch eine Mehrfachauswahl erstellt wurden, erhalten standardmäßig einen generischen Namen. Sobald ein Gerät registriert ist, ändert sich sein Name automatisch; ebenso die Hersteller- und Modell-Einträge.

3.7.4. GravityZone Mobile Client auf Geräten installieren

Die Anwendung GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

So installieren Sie GravityZone Mobile Client auf einem Gerät:

1. Suchen Sie die Anwendungen im offiziellen App-Store.
   - Link zu Google Play
   - Link zum Apple App Store
2. Laden Sie die Anwendung herunter, und installieren Sie sie auf dem Gerät.
3. Starten Sie die Anwendung, und nehmen Sie die nötige Konfiguration vor:
   a. Tippen Sie auf Android-Geräten auf **Aktivieren**, um GravityZone Mobile Client als Geräteadministrator zu aktivieren. Lesen Sie die Informationen gründlich durch.
   b. Geben Sie das Aktivierungs-Token und die Adresse des Kommunikationsservers ein, oder scannen Sie den QR-Code in der E-Mail ein.
   c. Tippen Sie auf **Aktivieren**.
   d. Auf iOS-Geräten werden Sie aufgefordert, das MDM-Profil zu installieren. Wenn ihr Gerät passwortgeschützt ist, werden Sie aufgefordert, das Passwort

einzugeben. Folgen Sie den Anweisungen auf Ihrem Bildschirm, um die Profilinstallation abzuschließen.

4. HILFE ERHALTEN

4.1. Verwenden des Support-Tools

Das Support-Tool von GravityZone ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Lösung von Problemen benötigen. Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Fehlersuche an einen Bitdefender-Support-Mitarbeiter.

4.1.1. Das Support-Tool unter Windows verwenden

1. Laden Sie das Support-Tool herunter und bringen Sie sie auf die betroffenen Computer aus. Um das Support-Tool herunterzuladen:
    a. Bauen Sie über Ihr Konto eine Verbindung mit der Control Center auf.
    b. Klicken Sie in der unteren linken Bildschirmecke der Konsole auf **Hilfe und Support**.
    c. Die Download-Links finden Sie im **Support**-Bereich. Es stehen zwei Versionen zur Verfügung: eine für 32-Bit-Systeme und eine für 64-Bit-Systeme. Stellen Sie sicher, dass Sie die richtige Version verwenden, wenn Sie das Support-Tool auf einem Computer ausführen.
2. Führen Sie das Support-Tool lokal auf jedem der betroffenen Computer aus.
    a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.
    b. Geben Sie in das Formular die nötigen Daten ein:
        i. Geben Sie Ihre E-Mail-Adresse ein.
        ii. Geben Sie Ihren Namen ein.
        iii. Wählen Sie Ihr Land aus dem entsprechenden Menü.
        iv. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.
        v. Sie können auch versuchen das Problem zu reproduzieren, bevor Sie mit der Datensammlung beginnen. Gehen Sie in diesem Fall folgendermaßen vor:
            A. Aktivieren Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**.

B. Klicken Sie auf **Weiter**.

C. Wählen Sie die Art des aufgetretenen Problems.

D. Klicken Sie auf **Weiter**.

E. Reproduzieren Sie das Problem auf Ihrem Computer. Kehren Sie danach zum Support-Tool zurück und wählen Sie die Option **Ich habe das Problem reproduziert**.

c. Klicken Sie auf **Weiter**. Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.

d. Warten Sie, bis der Vorgang beendet ist.

e. Klicken Sie auf **Beenden**, um das Fenster zu schließen. Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt.

   Schicken Sie das ZIP-Archiv gemeinsam mit Ihrer Anfrage an einen Bitdefender-Support-Mitarbeiter. Verwenden Sie dafür das E-Mail-Support-Ticket-Formular auf der **Hilfe und Support**-Seite der Konsole.

4.1.2. Das Support-Tool unter Linux

Für Linux-Betriebssysteme ist das Support-Tool im Bitdefender-Sicherheitsagenten integriert.

Linux-Systeminformationen können Sie über das Support-Tool mit dem folgendem Befehl erhalten:

```
# /opt/BitDefender/bin/bdconfigure
```

Dabei stehen folgende Optionen zur Verfügung:

- `--help` zeigt eine Liste aller Support-Tool-Befehle an.
- `enablelogs` aktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `disablelogs` deaktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `deliverall` erstellt ein Archiv, das die Produkt- und Kommunikationsmodulprotokolle enthält. Es wird an den Ordner `/tmp` im

folgenden Format zugestellt: `bitdefender_Maschinenname_Zeitstempel.tar.gz`.

1. Wenn Sie die Protokolle deaktivieren möchten, werden Sie um eine Bestätigung gebeten. Wenn nötig, werden die Dienste automatisch neu gestartet.
2. Wenn Sie Protokolle löschen möchten, werden Sie um eine Bestätigung gebeten.

- `deliverall -default` lLiefert dieselben Informationen wie die vorige Option, aber Standardaktionen werden auf die Protokolle ausgeführt, ohne dass der Benutzer dies bestätigt (die Protokolle werden deaktiviert und gelöscht).

So melden Sie ein GravityZone-Problem, das Ihre Linux-Systeme beeinträchtigt (verwenden Sie dazu die oben beschriebenen Optionen):

1. Aktivieren Sie Produkt- und Kommunikationsmodulprotokolle.
2. Versuchen Sie, das Problem nachzustellen.
3. Deaktivieren Sie Protokolle.
4. Erstellen Sie ein Protokollarchiv.
5. Öffnen Sie ein E-Mail-Support-Ticket über das Formular auf der Seite **Hilfe & Support** des Control Center; geben Sie eine Beschreibung des Problems ein und hängen Sie das Protokollarchiv an.

Das Support-Tool für Linux liefert die folgenden Informationen:

- Die Ordner `etc`, `var/log`, `/var/crash` (sofern vorhanden) und `var/epag` von `/opt/BitDefender`; darin sind die Bitdefender-Protokolle und -Einstellungen enthalten.
- Die Datei `/tmp/bdinstall.log`, die Installationsinformationen enthält.
- Die Datei `network.txt`, die Netzwerkeinstellungen und Informationen zur Netzwerkverbindung der Maschine enthält.
- Die Datei `system.txt`, die allgemeine Systeminformationen enthält (Distribution und Kernel-Version, verfügbarer RAM und freier Festplattenspeicher)
- Die Datei `users.txt`, die Benutzerinformationen enthält
- Andere Informationen zum Produkt im Zusammenhang mit dem Systen, z. B. externe Verbindungen von Prozessen und CPU-Auslastung

- Systemprotokolle